Cloud Computing Policy- Empanelment of Cloud Service Providers and Guidelines for Government organizations.

Government of Maharashtra
Directorate of Information Technology
Government Circular No. मातंसं - 060/3/2017/1
Hutatma Rajguru Chowk, Madam Cama Road,
Mantralaya, Mumbai – 400 032
Dated – 16th May, 2018

Introduction-

DIT vide its circular dated 29.1.2018, circulated the salient features of the Cloud Computing policy of the State and the operational instructions regarding the steps to be followed by the Departments.

As per para 4 of the above circular and approval of High Power Committee (IT) in its meeting held on 8.3.2018, DIT carried out a tendering process for empanelment of Cloud Service Providers (CSPs) and discovery of rates for various cloud services. Since this process has been duly completed now, it is necessary to issue detailed instructions regarding CSP empanelment and the action expected from the Government organizations to ensure that all IT applications are migrated to cloud by 30.10.2018. Accordingly, the following instructions are being issued by the Government.

Government Circular:-

1. The following Cloud service providers (CSP) are being hereby empanelled by DIT for a period of 3 years for providing cloud services to the all Government Departments, sub-ordinate offices, Public Sector Undertakings, Urban and Rural Local Bodies & any body/organization set up under any law of the State Government (henceforth collectively referred to as "Government organizations") from **1.5.2018 till 30.4.2021**.

   Tier-1 empanelment
   1. Amazon Web Services
   2. Microsoft
   3. Net Magic
   4. Control-S (Conditional Empanelment for Sec-A of Annexure 8.1, 8.2 and 8.3 and not any other section)

   Tier-2 empanelment
   1. ESDS

2. The total cumulative annual order value that can be awarded to CSPs in case of tier-2 empanelment will be subject to an upper cap of Rs 25 crore (inclusive of all Departments). Information regarding cumulative annual order value already awarded to tier-2 empanelled CSPs will be made available to Government organizations on a regular basis. Tier-1 has no upper or lower limit. Government organizations should ensure adherence to the upper cap limit at the time of selection of the CSP.

Cloud service offerings

3.1 The 3 cloud service offerings being provided by the empanelled CSPs are as follows.

   a) Public Cloud
   b) Virtual Private Cloud
   c) Government Community Cloud

3.2 As part of each of these cloud service offerings, the following cloud services will be available to Government organizations

- Virtual machines
- Storage
- Database
- Media transcoding
- Services like DNS, Active directory, Virtual Private Network (VPN), API management, email/SMS gateway, back-up services, mobile services, developer tools and office productivity tools
- Provision of Bare metal server as a service

Rates for cloud services

4.1 The details of the CSP empanelled for each offering (Public, Virtual Private Cloud and Government Community Cloud) and the services listed above and the applicable rates are provided in *Annexure-1.* The applicable rates for the offerings and services are different for tier-1 and tier-2 CSPs. These rates will be applicable from **1.5.2018 till 30.4.2020** after which fresh rates will be notified by DIT by following due process.

4.2. Three options- hourly rates, monthly rates if cloud services are taken for a minimum period of 1 year and monthly rates if cloud services are taken for a minimum period of 2 years are being made available to Government organizations.

4.3. If any Government organization has already hosted its IT application on the cloud of any of the CSPs being empanelled by this GR under any existing contract/work order with the CSP and if the rate for the cloud services as per the contract/work order is lower than the rates notified in *Annexure-1,* the rates specified in the existing work order/contract will apply till the term of that contract. However, if the existing contract/work order rates are higher, the rates notified in *Annexure-1* will apply from 1.5.2018. Foreclosure of Contract/work order can be done upto 31st October 2018.

4.4 If any Government organization has already hosted its IT application on the cloud of any other CSP not empanelled under this GR or for an offering/service for which the CSP is not empanelled under this GR, the IT application has to be migrated to a CSP empanelled under this GR before 30.10.2018.

4.5 To ensure that Government organizations get a hands-on experience, the Government organizations will be provided an option of free trial by the CSP for a limited period of 30 days before issue of formal work order.

Disaster Recovery (DR) services

5. Rates have been discovered for Datacenter services (DC only), Disaster Recovery (DR) services (DR only) and Datacenter & Disaster Recovery services (DC + DR). Government organizations may opt for one or more of these as per their requirements. If required, Government organizations may opt for different CSPs for DC and DR services.

Managed Service Providers (MSP)

6.1 A managed services provider (MSP) for this document is the cloud provider cloud services provider that manages and assumes responsibility for providing a defined set of services like Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) as per agreed term and conditions to Government organizations.

6.2 Each CSP may appoint a maximum of 2 Managed Service Providers (MSP). The CSP can function as its own MSP. The MSPs already appointed by the empanelled CSPs are listed in ***Annexure-1*****.** The MSP will perform the activities listed in ***Annexure-2*****.** Government organizations may opt for the migration services of MSPs in addition to the regular cloud offerings. If the Government organization decides to engage the migration services of the MSP, additional charges of **5%** (on the basic cloud services charges) towards MSP charges will apply for the period for which the services of MSP are engaged.

Selection of CSP

7. The Government organizations may select any of the empanelled CSPs through Departmental PC/PIC. Scope of work may be circulated to all empanelled CSP and presentation be done before PIC. After selection of the CSP, the Department may select any of the MSPs of the CSP, if required. If the Government organization has a system integrator or technical resource who can perform the technical tasks expected of a MSP, the Government organization can engage the system integrator or technical resource for performing the technical tasks instead of MSP.

Guidelines for selection of cloud offering

8.1 The following indicative guidelines should be used by Government organizations to decide the type of cloud offering (public cloud, virtual private cloud and Government community cloud) that they should opt for.

Sr.no	Type of IT application	Recommended cloud offering
1	Websites with only read access for citizens/users	Public Cloud
2	IT applications collecting and storing information regarding public infrastructure and public assets like roads, buildings, bridges, water bodies, water conservation structures, water supply and sanitation, telecom and IT networks etc. (including GIS) covered under RTI Act. Finance and Planning Departments regarding payment of taxes, revenue receipts.	Public Cloud
3	IT applications involving collection of taxes, revenue, user fees and charges for various G2B and G2C services and where personal sensitive information is NOT collected or stored	Virtual Private Cloud
4	IT applications involving collection and storage of information related to G2B services (Government to Business)	Virtual Private cloud
5	• IT applications involving collection and storage of information related to surveillance projects and safe and smart city projects in the State • Finance and Planning Departments regarding budget distribution, drawing and disbursement of Government funds	Virtual Private Cloud

6	Portals collecting and storing sensitive personal information of citizens like Aadhaar number, demographic data including address, date of birth, ekYC data, PAN number, Voter ID card number, bank account information, driving license information, personal health records (any one or more of the above)	Government Community Cloud
7	Irrespective of the above criteria, Applications of the following Departments • Property records of Revenue Department • Applications related to urban planning and development control regulations • Public Health Department & Medical Education Department- including health insurance and hospital management and information systems • School Education Department • Women and Child Development Department • Individual beneficiary schemes of Social Justice, Tribal Development, VJNT and OBC Department, Minorities Development and Skills Development Department • Food and Civil Supplies Department	Government Community Cloud

8.2 DIT may update and make necessary changes/additions in cloud guidelines for selection of cloud offerings from time to time.

8.3 It is clarified that the above cloud offering selection guidelines are indicative and Government organizations are free to choose the cloud service offering that would be suitable for them. While doing so, the Department should consider the nature and sensitivity of the data (in terms of data privacy, confidentiality, data concerning State & National security and requirements under the Right to Information Act) being handled by the application.

8.4 Departments to provide Cloud SPOC, Nodal officer and authorized signatory names in Scope of Work circulated to CSPs/MSP for cloud services.

Hosting/ Migration

9.1 If the Department engages a MSP, the MSP will submit a detailed plan regarding cloud deployment and configuration after carrying out a detailed study of the proposed/existing IT application of the Department. On acceptance of the above plan by the user Department, the MSP will assist the Department in deploying/migrating the Departmental application onto the cloud. The MSP must assist the Department in carrying out functional testing and data integrity testing to ensure operational acceptance. If the Department is engaging DR services, the MSP should carry out business continuity testing.

9.2 All Government organizations must ensure that all existing applications are migrated to cloud on or before **30.10.2018**.

Payments linked to utilization

10.1 In the case of cloud services provisioned by user Government organizations, the billing for cloud services will be based on actual consumption of services (Pay-As-You-Go model) with zero capital (one- time) cost.

10.2 To incentivize optimal solution design and encourage proper utilization of the assigned computing resources, empanelled CSP in co-ordination with the user Department should ensure that the average monthly utilization of RAM, CPU and storage is not less than **50%**. If the average monthly utilization is less than 50% in a particular month, the CSP should

immediately notify the user Department. The user Department and the MSP/CSP should undertake a joint assessment within 15 days, analyze the reasons for the utilization being less than 50% and undertake steps to ensure resource utilization of at least 50%. If the average monthly utilization of RAM or CPU or storage is less than 50% for 2 successive months, a penalty of **25%** of the monthly bill amount (from the next billing cycle) will apply for those particular months where utilization is below 50%.

However, if the CSP has proposed a resource optimization plan to bring the average utilization above 50% but such plan has not been approved by the user Department authorized Signatory within the above time period of 2 months, the penalty will be waived off by DIT.

10.3 If average monthly utilization exceeds **65%**, an additional incentive of **5%** of the monthly bill amount will be payable to the CSP for a period not exceeding 6 months. The expenditure towards cloud services will be borne by the user Department from their budgetary resources. It is clarified that DIT will not bear the expenditure centrally for availing cloud services. Empanelled Cloud Service providers will raise quarterly invoices to the respective Department. Payments should ordinarily be made by the respective user Department within 1 month of the raising of the invoice.

Management / Transition-Out Services

11. CSP will provide a comprehensive exit management plan, with focus on sustainability and do Migration of the VMs, data, content and any other assets to the new environment or on alternate Managed Service Provider's offerings and ensuring successful deployment and running of user Department's solution on the new infrastructure by suitably retrieving all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to Agency supplied industry standard media.

12. CSP Ensure that all the documentation required for smooth transition including configuration documents are kept up to date. Once the exit process is completed, remove the data, content and other assets from the cloud environment and destroy the VM, Content and data of user Department.

Performance Bank Guarantee

13. In addition to a one-time performance bank guarantee (PBG) of Rs. 50 lakhs to be submitted by empanelled CSPs to DIT for the entire duration of this empanelment, a PBG of 10% of the contract value should be submitted by MSP/CSP to respective user Department for the period of the work order, if work order value exceeds Rs. 5 lakhs in a financial year. Any penalties as per the Service Level Agreements (SLAs) may be recovered from this PBG.

This Government Circular of Maharashtra Government is available at the website www.maharashtra.gov.in Reference no. for this is 201805171357566211. This order has been signed digitally.

By order and in the name of the Governor of Maharashtra,

S V R Srinivas

Digitally signed by S V R Srinivas
DN: c=IN, postalCode=400020, st=Maharashtra, 2.5.4.20=31d35fda97cba0c6a6c5e2ca7125fd8ba7f7201a47f0e71dbf230047862bd061, serialNumber=914d8a9c1092ca4b44280033c71560ea75b2d56dcb4d3fc1f81eb6dfc5fcbe63, cn=S V R Srinivas
Date: 2018.05.17 15:00:30 +05'30'

(S.V.R. Srinivas)
Principal Secretary IT,
Government of Maharashtra.

Copy forwarded to:

1) Secretary to the Hon'ble Governor of Maharashtra

2) Secretary to Hon'ble Chief Minister,
3) Personal Secretary to All Ministers/All Ministers of State,
4) Hon'ble Leader of Opposition, Legislative Assembly/ Legislative council, Maharashtra Vidhan Mandal Sachiwalaya, Mumbai,
5) All Hon'ble Members of Legislative Assembly/ Legislative Council,
6) Personal Assistant to Chief Secretary,
7) Additional Chief Secretary/Principal Secretary/Secretary of All Departments,
8) Registrar, High Court (Original Side) Mumbai,
9) Registrar, High Court (Appellate Side) Mumbai,
10) Registrar, Lok Ayukta and Up Lok Ayukta, Maharashtra State Mumbai,
11) Secretary State Election Commission, Mumbai
12) Secretary, Maharashtra Public Service Commission Mumbai,
13) Principal Secretary, Maharashtra Vidhan Mandal Sachiwalaya Mumbai,
14) Chief Information Commissioner, State Information Commission, Mumbai,
15) Auditor, Accountant General (A & E), Maharashtra Mumbai,
16) Auditor, Accountant General (A & E), Maharashtra Nagpur,
17) Auditor, Accountant General (Audit), Maharashtra Mumabai,
18) Auditor, Accountant General (Audit), Maharashtra Nagpur,
19) Pay and Accounts Officer, Mumbai,
20) Residential Audit Officer, Mumbai,
21) Commissioners of All Municipal Corporations,
22) All Collectors,
23) All Chief Executive Officer, Zilla Parishad/ All Chief Officers,
24) Director General, Information and Public Relations, Mantralaya Mumbai,
25) Managing Director, Maharashtra IT Corporation Mumbai,
26) Select File, DIT, General Administration Department, Mantralaya.

Annexure 1

Public Cloud

Line Item #	Sec-A	Line Items			DC-Public Cloud 1 year		DR-Public Cloud 1 year		DC+DR-Public Cloud 1 year	
	VM	cpu	RAM	Storage (GB)	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate
1	Pack 1	1	1	50	2.5	1800.0	**2.3**	**1626.0**	15.20	11153.00
2	Pack 2	1	2	100	3.0	2160.0	**2.7**	**1956.0**	19.00	13961.20
3	Pack 3	2	4	100	6.0	4320.0	**5.4**	**3912.0**	31.36	22972.90
4	Pack 4	2	8	150	8.0	5760.0	**7.2**	**5232.0**	41.00	28955.00
5	Pack 5	2	16	150	12.0	8640.0	10.8	7872.0	44.00	30989.00
6	Pack 6	4	4	200	10.0	7200.0	9.0	6504.0	69.00	49565.00
7	Pack 7	4	8	250	12.0	8640.0	10.8	7824.0	69.00	49565.00
8	Pack 8	4	16	250	16.0	11520.0	14.4	10464.0	69.00	51431.00
9	Pack 9	6	6	300	15.0	10800.0	13.5	9756.0	72.00	97917.00
10	Pack 10	6	12	350	18.0	12960.0	16.2	11736.0	137.00	98899.00
11	Pack 11	8	8	400	20.0	14400.0	18.0	13008.0	137.00	98899.00
12	Pack 12	8	16	450	24.0	17280.0	21.6	15648.0	137.00	98899.00
13	Pack 13	8	32	450	32.0	23040.0	28.8	20928.0	127.68	93474.30
14	Pack 14	12	12	500	30.0	21600.0	27.0	19512.0	260.42	175000.75
15	Pack 15	12	24	550	36.0	25920.0	32.4	23472.0	262.55	176432.37
16	Pack 16	16	16	600	40.0	28800.0	36.0	26016.0	264.68	177863.98
17	Pack 17	16	32	650	48.0	34560.0	43.2	31296.0	266.81	179295.59
18	Pack 18	32	64	700	96.0	69120.0	86.4	62592.0	575.71	386879.33
19	Pack 19	64	128	750	192.0	138240.0	172.8	125184.0	1081.83	726992.67
20	Pack 20	128	256	800	2517.5	1843053.2	2517.5	1843053.2	5035.00	3686106.40
21	Bandwidth-Plan 1- upto 100 GB					754.0				
22	Bandwidth-Plan 2- upto 500 GB					3927.0				
23	Bandwidth-Plan 3- upto 1000 GB					8000.0				
24	Additional data transfer tariff per GB					8.0				

Line Item #	SEC- B STORAGE	Line Items		MONTHLY rate
25	Object storage	50 GB		118.75
26		500 GB		737.00
27		1000 GB		1,398.00
28		10 TB		13,613.00
29	File storage	50 GB		141.00
30		500 GB		1,406.00
31		1000 GB		2,813.00
32		10 TB		25,571.00
33	Archive storage	50 GB		10.00

34		500 GB		237.50
35		1000 GB		475.00
36		10 TB		4,864.00
37	DISK storage	50 GB	<= 120 IOPS	125.00
38			121 to 400 IOPS	243.00
39			401 to 800 IOPS	625.00
40			801 to 1200 IOPS	800.00
41			1201 to 2000 IOPS	1,125.00
42			> 5000 IOPS	2,000.00
43		500 GB	<= 120 IOPS	1,250.00
44			121 to 400 IOPS	1,696.00
45			401 to 800 IOPS	1,696.00
46			801 to 1200 IOPS	1,808.00
47			1201 to 2000 IOPS	1,944.00
48			> 5000 IOPS	7,727.00
49		1000 GB	<= 120 IOPS	2,500.00
50			121 to 400 IOPS	3,212.00
51			401 to 800 IOPS	3,212.00
52			801 to 1200 IOPS	3,392.00
53			1201 to 2000 IOPS	3,616.00
54			> 5000 IOPS	8,035.00
55		10 TB	<= 120 IOPS	25,000.00
56			121 to 400 IOPS	29,828.00
57			401 to 800 IOPS	29,828.00
58			801 to 1200 IOPS	29,828.00
59			1201 to 2000 IOPS	29,828.00
60			> 5000 IOPS	44,011.00

Line Item #	SEC-C DATABASE	Database Options	No. of Licenses required		MONTHLY rate
61	Postgre Enterprise		4		34,868.63
62			5 to 8		69,639.04
63			> 8		153,421.98
64	MySQL 4 socket, 8 socket, 16 socket and 32 socket		4 socket		11,826.00
65			8 socket		23,645.00
66			16 socket		47,290.00
67			32 socket		94,572.00
68	MySQL Standard		4		-
69			5 to 8		-
70			> 8		-
71	MySQL Enterprise		4		-
72			5 to 8		-
73			> 8		-
74	MSSQL 2012 Standard		4		21,976.00
75			5 to 8		43,952.00

76			> 8		87,904.00
77	MSSQL 2012 Enterprise		4		84,270.00
78			5 to 8		168,540.00
79			> 8		337,080.00
80	Oracle Standard		4		70,817.70
81			5 to 8		155,907.12
82			> 8		311,165.71
83	Oracle Enterprise		4		-
84			5 to 8		-
85			> 8		-
86	NoSQL Enterprise		100		2,859.50
87			101 to 500		14,297.50
88			501 to 1000		28,595.00
89			> 1000		4,049.96
90	IBM DB2 v 10.5 or above		2		-
91			4		-
92			10		-
93			> 10		-
94	NoSQL DB		100		2,859.50
95			101 to 500		14,297.50
96			501 to 1000		28,595.00
97			> 1000		28,595.00
98	MySQL & Postgre SQL compatible relational database		4		42,628.13
99			5 to 8		85,354.48
100			> 8		170,610.75
SEC-D		**Media transcoding at 99.9% availability**			**MONTHLY rate**
		Quality	Multiplier		-
101		SD(1280X720)	1X	per output minute	1.90
102		HD (1280 × 720–1920 x 1080	2X	per output minute	2.85
103		UHD (more than 1920 x 1080, up to 4096 x 2160)	4X	per output minute	10.06
104		Audio only output	0.25X	per output minute	0.95
Line Item #	**SEC-E SERVICES**				**MONTHLY rate**
105	**Scalability**	Virtual Machine Scale Sets/Auto Scaling		1 unit of 5 VMs	3,000.00

106	**DNS**	DNS Management	1	51.30
107	**AD**	Active Directory Services	1	5,000.00
108	**VPN**	VPN/Gateway SITE to SITE point to point	2 ports per VPN	1,045.00
109	**API Gateway/ Management**	Million API calls	1	332.50
110	**Email/SMS**	Email gateway	Per year cost for 1 account with 10 GB	60.00
111		SMS gateway	1 lakh sms per month	16,720.00
112	**Public IP**	Additional public IP Addresses	1	100.00
113	**DASHBOARDS**	Network Monitoring dash Board	1	1,000.00
114	**BACKUP Services**	Backup agent , Backup management and monitoring , Back up Restoration	1	600.00
115	**DATA TRANSFER**	Bulk Data Transfer	1 TB	7,931.55
116		DATA SYNC service	1 TB	5,000.00
117	**Developer Tools**	Tools & SDKs or equivalent	1 instance	16,525.00
118		Code Deploy and commit tools or equivalent	1 instance	95.00
119	**Mobile Services**	Mobile Hub or equivalent	1	93,936.00
120		Mobile SDK	1	-
121		Container /Registry	1	9.50
122	Office 365(Email Service with 100 GB Mail Box each for primary and archival, Multiparty Video conferencing on PC, Laptop and tablets, personal data storage sync from PC to cloud, office productivity , search capabilities) or equivalent		1	-
Line Item #	**SEC- F**	**Bare Metal Servers**		MONTHLY rate
123	Intel Xeon E7-8890 v4 (192 Cores, 2.20 GHz),8192GB RAM (8192GB maximum), Up to 29 Internal Hard Drives Up to 10Gbps maximum Port Speeds, Redundant Power Supplies, Hypervisor Licenses, network connectivity to internet or Cloud infrastructure		1	1,174,281.89
124	Quad Intel Xeon E7-4890 v2 (60 Cores, 2.80 GHz) 2048GB RAM (2048GB maximum) Up to 24 Internal Hard Drives Up to 10Gbps maximum Port Speeds Redundant Power Supplies Hypervisor Licenses, network connectivity to internet or Cloud infrastructure		1	391,427.30
125	Intel Xeon E5-2690 v4, Dual Intel Xeon E5-2690 v4 (28 Cores, 2.60 GHz) 256GB RAM (256GB maximum) Up to 2 Internal Hard Drives Up to 10Gbps maximum Port Speeds Redundant Power Supplies Hypervisor Licenses, network connectivity to internet or Cloud infrastructure		1	88,071.14
Line Item #	Section G	Data transfer allowed per month		MONTHLY rate
	Additional resources			-
130	1 Virtual CPU			450.00
126	1 GB RAM			220.00
127	Storage in minimum block of 50 GB			243.00
128	Additional network segment (per VLAN)			-

129	Additional 1 IP			100.00
130	Additional 1 sub-admin account			500.00
	MSP Charges			
131	MSP Charges			5%

Line Item #	Sec-A	Line Items			DC-Public Cloud 2 year		DR-Public Cloud 2 year		DC+DR-Public Cloud 2 year	
1	VM	cpu	RAM	Storage (GB)	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate
2	Pack 1	1	1	50	2.5	1730.0	2.3	1550.0	15.2	10472.8
3	Pack 2	1	2	100	3.0	2060.0	2.7	1850.0	19.0	12638.8
4	Pack 3	2	4	100	6.0	4120.0	5.4	3700.0	31.4	14774.4
5	Pack 4	2	8	150	8.0	5440.0	7.2	4900.0	41.0	20641.6
6	Pack 5	2	16	150	12.0	8080.0	10.8	7300.0	44.0	29727.4
7	Pack 6	4	4	200	10.0	6920.0	9.0	6200.0	69.0	47315.7
8	Pack 7	4	8	250	12.0	8240.0	10.8	7400.0	69.0	48412.0
9	Pack 8	4	16	250	16.0	10880.0	14.4	9800.0	71.3	34819.4
10	Pack 9	6	6	300	15.0	10380.0	13.5	9300.0	135.0	92353.3
11	Pack 10	6	12	350	18.0	12360.0	16.2	11100.0	137.0	93436.3
12	Pack 11	8	8	400	20.0	13840.0	18.0	12400.0	137.0	94519.3
13	Pack 12	8	16	450	24.0	16480.0	21.6	14800.0	137.0	95602.3
14	Pack 13	8	32	450	32.0	21760.0	28.8	19600.0	127.7	62591.7
15	Pack 14	12	12	500	30.0	20760.0	27.0	18600.0	260.4	162500.7
16	Pack 15	12	24	550	36.0	24720.0	32.4	22200.0	262.6	163830.1
17	Pack 16	16	16	600	40.0	27680.0	36.0	24800.0	264.7	165159.4
18	Pack 17	16	32	650	48.0	32960.0	43.2	29600.0	266.8	166488.8
19	Pack 18	32	64	700	96.0	65920.0	86.4	59200.0	575.7	359245.1
20	Pack 19	64	128	750	192.0	131840.0	172.8	118400.0	1081.8	675064.6
21	Pack 20	128	256	800	2517.5	1314756.3	2517.5	1314756.3	5035.0	2629512.6
22	Bandwidth-Plan 1- upto 100 GB					754.00				
23	Bandwidth-Plan 2- upto 500 GB					3,927.00				
24	Bandwidth-Plan 3- upto 1000 GB					8,000.00				
25	Additional data transfer tariff per GB					8.00				

Virtual Private Cloud

Line Item #	Sec-A	Line Items			

Government Circular No.: **मातंसं - 060/3/2017/1**

1	VM	cpu	RAM	Storage (GB)	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate
2	Pack 1	1	1	50	10.00	6,621.00	10.00	7231.00	20.00	13852.00
3	Pack 2	1	2	100	10.00	6,830.00	10.00	7421.00	21.00	14251.00
4	Pack 3	2	4	100	16.00	11,569.00	16.00	13267.00	35.00	24836.00
5	Pack 4	2	8	150	21.00	14,596.00	21.00	14359.00	41.00	28955.00
6	Pack 5	2	16	150	21.00	14,830.00	21.00	16159.00	44.00	30989.00
7	Pack 6	4	4	200	32.00	23,081.00	32.00	26484.00	69.00	49565.00
8	Pack 7	4	8	250	32.00	23,081.00	32.00	26484.00	69.00	49565.00
9	Pack 8	4	16	250	36.00	25,753.00	36.00	25678.00	69.00	51431.00
10	Pack 9	6	6	300	63.00	45,505.00	63.00	52412.00	72.00	97917.00
11	Pack 10	6	12	350	64.00	46,020.00	64.00	52879.00	137.00	98899.00
12	Pack 11	8	8	400	64.00	46,020.00	64.00	52879.00	137.00	98899.00
13	Pack 12	8	16	450	64.00	46,020.00	64.00	52879.00	137.00	98899.00
14	Pack 13	8	32	450	71.00	51,407.00	71.00	56240.00	149.00	107647.00
15	Pack 14	12	12	500	124.00	90,372.00	124.00	104236.00	267.00	194608.00
16	Pack 15	12	24	550	125.00	90,616.00	125.00	104459.00	269.00	195075.00
17	Pack 16	16	16	600	125.00	88,768.00	125.00	104649.00	269.00	193417.00
18	Pack 17	16	32	650	125.00	90,824.00	125.00	104649.00	269.00	195473.00
19	Pack 18	32	64	700	276.00	201,235.00	276.00	220973.00	579.00	422208.00
20	Pack 19	64	128	750	550.00	400,808.00	550.00	440429.00	1154.00	841237.00
21	Pack 20	128	256	800	0.00	-	0.00	0.00	0.00	0.00
22	Bandwidth-Plan 1- upto 100 GB					754.00				
23	Bandwidth-Plan 2- upto 500 GB					3,927.00				
24	Bandwidth-Plan 3- upto 1000 GB					8,083.00				
25	Additional data transfer tariff per GB					8.00				

Line Item #	SEC- B STORAGE		Line Items	HOURLY rate	MONTHLY rate
26	Object storage	50 GB		0.00	125.00
27		500 GB		0.00	737.00
28		1000 GB		0.00	1,398.00
29		10 TB		0.00	13,613.00
30	File storage	50 GB		0.00	141.00

31		500 GB		0.00	1,406.00
32		1000 GB		0.00	2,813.00
33		10 TB		0.00	25,571.00
34	Archive storage	50 GB		0.00	117.00
35		500 GB		0.00	698.00
36		1000 GB		0.00	978.00
37		10 TB		0.00	8,258.00
38	DISK storage	50 GB	<= 120 IOPS	0.00	125.00
39			121 to 400 IOPS	0.00	243.00
40			401 to 800 IOPS	0.00	625.00
41			801 to 1200 IOPS	0.00	800.00
42			1201 to 2000 IOPS	0.00	1,125.00
43			> 5000 IOPS	0.00	2,000.00
44		500 GB	<= 120 IOPS	0.00	1,250.00
45			121 to 400 IOPS	0.00	1,696.00
46			401 to 800 IOPS	0.00	1,696.00
47			801 to 1200 IOPS	0.00	1,808.00
48			1201 to 2000 IOPS	0.00	1,944.00
49			> 5000 IOPS	0.00	7,727.00
50		1000 GB	<= 120 IOPS	0.00	2,500.00
51			121 to 400 IOPS	0.00	3,212.00
52			401 to 800 IOPS	0.00	3,212.00
53			801 to 1200 IOPS	0.00	3,392.00
54			1201 to 2000 IOPS	0.00	3,616.00
55			> 5000 IOPS	0.00	8,035.00
56		10 TB	<= 120 IOPS	0.00	25,000.00

57			121 to 400 IOPS	0.00	29,828.00
58			401 to 800 IOPS	0.00	29,828.00
59			801 to 1200 IOPS	0.00	29,828.00
60			1201 to 2000 IOPS	0.00	29,828.00
61			> 5000 IOPS	0.00	44,011.00
Line Item #	**SEC-C DATABASE**	**Database Options**	**No. of Licenses required**	**HOURLY rate**	**MONTHLY rate**
62		Postgre Enterprise	4	0.00	-
63			5 to 8	0.00	-
64			> 8	0.00	-
65		MySQL 4 socket, 8 socket, 16 socket and 32 socket	4 socket		11,826.00
66			8 socket		23,645.00
67			16 socket		47,290.00
68			32 socket		94,572.00
69		MySQL Standard	4	0.00	-
70			5 to 8	0.00	-
71			> 8	0.00	-
72		MySQL Enterprise	4	0.00	-
73			5 to 8	0.00	-
74			> 8	0.00	-
75		MSSQL 2012 Standard	4	0.00	21,976.00
76			5 to 8	0.00	43,952.00
77			> 8	0.00	87,904.00
78		MSSQL 2012 Enterprise	4	0.00	84,270.00
79			5 to 8	0.00	168,540.00
80			> 8	0.00	337,080.00

81		Oracle Standard	4		0.00	-
82			5 to 8		0.00	-
83			> 8		0.00	-
84		Oracle Enterprise	4		0.00	-
85			5 to 8		0.00	-
86			> 8		0.00	-
87		NoSQL Enterprise	100		0.00	-
88			101 to 500		0.00	-
89			501 to 1000		0.00	-
90			> 1000		0.00	-
91		IBM DB2 v 10.5 or above	2		0.00	-
92			4		0.00	-
93			10		0.00	-
94			> 10		0.00	-
95		NoSQL DB	100		0.00	-
96			101 to 500		0.00	-
97			501 to 1000		0.00	-
98			> 1000		0.00	-
99	MySQL & Postgre SQL compatible relational database		4		0.00	-
100			5 to 8		0.00	-
101			> 8		0.00	-
	SEC-D	**Media transcoding at 99.9% availibility**			**HOURLY AMT**	**MONTHLY AMT**
		Quality	Multiplier			-
102		SD(1280X720)	1X	per out put minute	0.00	2.98
103		HD (1280 × 720–1920 x 1080	2X	per out put minute	0.00	5.29

104		UHD (more than 1920 x 1080, up to 4096 x 2160)	4X	per out put minute	0.00	10.06
105		Audio only output	0.25X	per out put minute	0.00	2.98
Line Item #				SEC-E SERVICES	HOURLY rate	MONTHLY rate
106	Scalability	Virtual Machine Scale Sets/Auto Scaling		1 unit of 5 VMs	0.00	-
107	DNS	DNS Management		1	0.00	2,975.00
108	AD	Active Directory Services		1	0.00	5,000.00
109	VPN	VPN/Gateway SITE to SITE point to point		2 ports per VPN	0.00	4,000.00
110	API Gateway/ Management	Million API calls		1	0.00	332.50
111	Email/SMS	Email gateway		Per year cost for 1 account with 10 GB	0.00	60.00
112		SMS gateway		1 lakh sms per month	0.00	17,000.00
113	Public IP	Additional public IP Addresses		1	0.00	125.00
114	DASHBOARDS	Network Monitoring dash Board		1	0.00	1,000.00
115	BACKUP Services	Backup agent , Backup management and monitoring , Back up Restoration		1	0.00	1,322.00
116	DATA TRANSFER	Bulk Data Transfer		1 TB	0.00	7,931.55
117		DATA SYNC service		1 TB	0.00	5,000.00
118	Developer Tools	Tools & SDKs or equivalent		1 instance	0.00	16,525.00
119		Code Deploy and commit tools or equivalent		1 instance	0.00	95.00
120	Mobile Services	Mobile Hub or equivalent		1	0.00	93,936.00
121		Mobile SDK		1	0.00	-
122		Container /Registry		1	0.00	3,305.00
124	Office 365(Email Service with 100 GB Mail Box each for primary and archival, Multiparty Video conferencing on PC, Laptop and tablets, personal data storage sync from PC to cloud, office productivity , search capabilities) or equivalent			1	-	-
Line Item #	SEC- F	Bare Metal Servers				
					HOURLY rate	MONTHLY rate
125	Intel Xeon E7-8890 v4 (192 Cores, 2.20 GHz),8192GB RAM (8192GB maximum), Up to 29 Internal Hard Drives Up to 10Gbps maximum Port Speeds, Redundant			1	0.00	1,174,281.89

	Power Supplies, Hypervisor Licenses, network connectivity to internet or Cloud infrastructure					
126	Quad Intel Xeon E7-4890 v2 (60 Cores, 2.80 GHz) 2048GB RAM (2048GB maximum) Up to 24 Internal Hard Drives Up to 10Gbps maximum Port Speeds Redundant Power Supplies Hypervisor Licenses, network connectivity to internet or Cloud infrastructure			1	0.00	391,427.30
127	Intel Xeon E5-2690 v4, Dual Intel Xeon E5-2690 v4 (28 Cores, 2.60 GHz) 256GB RAM (256GB maximum) Up to 2 Internal Hard Drives Up to 10Gbps maximum Port Speeds Redundant Power Supplies Hypervisor Licenses, network connectivity to internet or Cloud infrastructure			1	0.00	88,071.14
	Section G	Data transfer allowed per month				
Line Item #					HOURLY rate	MONTHLY rate
	Additional resources				0.00	-
128		1 Virtual CPU			0.00	500.00
129		1 GB RAM			0.00	50.00
130		Storage in minimum block of 50 GB			0.00	10.00
131		Additional network segment (per VLAN)			0.00	100.00
132		Additional 1 IP			0.00	125.00
133		Additional 1 sub-admin account			0.00	500.00
134	MSP Charges	5%				

Line Item #	Sec-A	Line Items			DC-Virtual Public Cloud 2 year		DR-Virtual Public Cloud 2 year		DC+DR-Virtual Public Cloud 2 year	
1	**VM**	**cpu**	**RAM**	**Storage (GB)**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**
2	Pack 1	1	1	50	10.00	6,621.00	10.00	7,231.00	20	13852
3	Pack 2	1	2	100	10.00	6,830.00	10.00	7,421.00	21	14251
4	Pack 3	2	4	100	16.00	11,569.00	16.00	13,267.00	35	24836
5	Pack 4	2	8	150	21.00	14,596.00	21.00	14,359.00	41	28955
6	Pack 5	2	16	150	21.00	14,830.00	21.00	16,159.00	44	30989
7	Pack 6	4	4	200	32.00	23,081.00	32.00	26,484.00	69	49565
8	Pack 7	4	8	250	32.00	23,081.00	32.00	26,484.00	69	49565
9	Pack 8	4	16	250	36.00	25,753.00	36.00	25,678.00	72	51431
10	Pack 9	6	6	300	63.00	45,505.00	63.00	52,412.00	135	97917
11	Pack 10	6	12	350	64.00	46,020.00	64.00	52,879.00	137	98899
12	Pack 11	8	8	400	64.00	46,020.00	64.00	52,879.00	137	98899
13	Pack 12	8	16	450	64.00	46,020.00	64.00	52,879.00	137	98899

14	Pack 13	8	32	450	71.00	51,407.00	71.00	56,240.00	149	107647
15	Pack 14	12	12	500	124.00	90,372.00	124.00	104,236.00	267	194608
16	Pack 15	12	24	550	125.00	90,616.00	125.00	104,459.00	269	195075
17	Pack 16	16	16	600	125.00	88,768.00	125.00	104,649.00	269	193417
18	Pack 17	16	32	650	125.00	90,824.00	125.00	104,649.00	269	195473
19	Pack 18	32	64	700	276.00	201,235.00	276.00	220,973.00	579	422208
20	Pack 19	64	128	750	550.00	400,808.00	550.00	440,429.00	1154	841237
21	Pack 20	128	256	800	0.00	-	0.00	-	0	0
22	Bandwidth-Plan 1- upto 100 GB					754.00				
23	Bandwidth-Plan 2- upto 500 GB					3,927.00				
24	Bandwidth-Plan 3- upto 1000 GB					8,083.00				
25	Additional data transfer tariff per GB					8.00				

Government Community Cloud

Line Item #	Sec-A	Line Items			DC-Government Community Cloud 1 year		DR-Government Community Cloud 1 year		DC+DR-Government Community Cloud 1 year	
1	**VM**	**cpu**	**RAM**	**Storage (GB)**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**
2	Pack 1	1	1	50	14.00	9,269.40	14.00	10,123.40	28.00	19,392.80
3	Pack 2	1	2	100	14.00	9,562.00	15.40	10,389.40	29.40	19,951.40
4	Pack 3	2	4	100	22.40	16,196.60	26.60	18,573.80	49.00	34,770.40
5	Pack 4	2	8	150	29.40	20,434.40	28.00	20,102.60	57.40	40,537.00
6	Pack 5	2	16	150	29.40	20,762.00	32.20	22,622.60	61.60	43,384.60
7	Pack 6	4	4	200	44.80	32,313.40	51.80	37,077.60	96.60	69,391.00
8	Pack 7	4	8	250	44.80	32,313.40	51.80	37,077.60	96.60	69,391.00
9	Pack 8	4	16	250	50.40	36,054.20	50.40	35,949.20	100.80	72,003.40

10	Pack 9	6	6	300	88.20	63,707.00	100.80	73,376.80	189.00	137,083.80
11	Pack 10	6	12	350	89.60	64,428.00	102.20	74,030.60	191.80	138,458.60
12	Pack 11	8	8	400	89.60	64,428.00	102.20	74,030.60	191.80	138,458.60
13	Pack 12	8	16	450	89.60	64,428.00	102.20	74,030.60	191.80	138,458.60
14	Pack 13	8	32	450	99.40	71,969.80	109.20	78,736.00	208.60	150,705.80
15	Pack 14	12	12	500	173.60	126,520.80	200.20	145,930.40	373.80	272,451.20
16	Pack 15	12	24	550	175.00	126,862.40	201.60	146,242.60	376.60	273,105.00
17	Pack 16	16	16	600	175.00	124,275.20	244.80	146,508.60	457.30	270,783.80
18	Pack 17	16	32	650	175.00	127,153.60	201.60	146,508.60	376.60	273,662.20
19	Pack 18	32	64	700	386.40	281,729.00	424.20	309,362.20	810.60	591,091.20
20	Pack 19	64	128	750	770.00	561,131.20	845.60	748,729.30	1,615.60	1,177,731.80
21	Pack 20	128	256	800	-	-	-	-	-	-
22	Bandwidth-Plan 1- upto 100 GB					754.00				
23	Bandwidth-Plan 2- upto 500 GB					3,927.00				
24	Bandwidth-Plan 3- upto 1000 GB					8,083.00				
25	Additional data transfer tariff per GB					8.00				

Line Item #	SEC- B STORAGE	Line Items			HOURLY rate	MONTHLY rate
26	Object storage		50 GB		-	125.00
27			500 GB		-	737.00
28			1000 GB		-	1,398.00
29			10 TB		-	13,613.00
30	File storage		50 GB		-	141.00

31		500 GB		-	1,406.00
32		1000 GB		-	2,813.00
33		10 TB		-	25,571.00
34	Archive storage	50 GB		-	117.00
35		500 GB		-	698.00
36		1000 GB		-	978.00
37		10 TB		-	8,258.00
38	DISK storage	50 GB	<= 120 IOPS	-	125.00
39			121 to 400 IOPS	-	243.00
40			401 to 800 IOPS	-	625.00
41			801 to 1200 IOPS	-	800.00
42			1201 to 2000 IOPS	-	1,125.00
43			> 5000 IOPS	-	2,000.00
44		500 GB	<= 120 IOPS	-	1,250.00
45			121 to 400 IOPS	-	1,696.00
46			401 to 800 IOPS	-	1,696.00
47			801 to 1200 IOPS	-	1,808.00
48			1201 to 2000 IOPS	-	1,944.00
49			> 5000 IOPS	-	7,727.00
50		1000 GB	<= 120 IOPS	-	1,662.60
51			121 to 400 IOPS	-	3,212.00
52			401 to 800 IOPS	-	3,212.00
53			801 to 1200 IOPS	-	3,392.00
54			1201 to 2000 IOPS	-	3,616.00
55			> 5000 IOPS	-	8,035.00
56		10 TB	<= 120 IOPS	-	25,000.00

57			121 to 400 IOPS	-	29,828.00
58			401 to 800 IOPS	-	29,828.00
59			801 to 1200 IOPS	-	29,828.00
60			1201 to 2000 IOPS	-	29,828.00
61			> 5000 IOPS	-	44,011.00
Line Item #	**SEC-C DATABASE**	**Database Options**	**No. of Licenses required**	**HOURLY rate**	**MONTHLY rate**
62	Postgre Enterprise		4	-	-
63			5 to 8	-	-
64			> 8	-	-
65	MySQL 4 socket, 8 socket, 16 socket and 32 socket		4 socket		16,556.40
66			8 socket		33,103.00
67			16 socket		66,206.00
68			32 socket		132,400.80
69	MySQL Standard		4	-	-
70			5 to 8	-	-
71			> 8	-	-
72	MySQL Enterprise		4	-	-
73			5 to 8	-	-
74			> 8	-	-
75	MSSQL 2012 Standard		4	-	21,976.00
76			5 to 8	-	43,952.00
77			> 8	-	87,904.00
78	MSSQL 2012 Enterprise		4	-	84,270.00
79			5 to 8	-	168,540.00
80			> 8	-	337,080.00

81	Oracle Standard		4		-	-
82			5 to 8		-	-
83			> 8		-	-
84	Oracle Enterprise		4		-	-
85			5 to 8		-	-
86			> 8		-	-
87	NoSQL Enterprise		100		-	-
88			101 to 500		-	-
89			501 to 1000		-	-
90			> 1000		-	-
91	IBM DB2 v 10.5 or above		2		-	-
92			4		-	-
93			10		-	-
94			> 10		-	-
95	NoSQL DB		100		-	-
96			101 to 500		-	-
97			501 to 1000		-	-
98			> 1000		-	-
99	MySQL & Postgre SQL compatible relational database		4		-	-
100			5 to 8		-	-
101			> 8		-	-
SEC-D		**Media transcoding at 99.9% availability** Quality	Multiplier		**HOURLY AMT**	**MONTHLY AMT**
102		SD(1280X720)	1X	per output minute	-	4.17
103		HD (1280 × 720–1920 x 1080	2X	per output minute	-	7.41
104		UHD (more than 1920 x 1080, up to 4096 x 2160)	4X	per output minute	-	13.89

105		Audio only output	0.25X	per output minute	-	4.17
Line Item #	SEC-E SERVICES				HOURLY rate	MONTHLY rate
106	Scalability	Virtual Machine Scale Sets/Auto Scaling		1 unit of 5 VMs	-	-
107	DNS	DNS Management		1	-	2,975.00
108	AD	Active Directory Services		1	-	5,000.00
109	VPN	VPN/Gateway SITE to SITE point to point		2 ports per VPN	-	4,000.00
110	API Gateway / Management	Million API calls		1	-	258,648.60
111	Email/SMS	Email gateway		Per year cost for 1 account with 10 GB	-	60.00
112		SMS gateway		1 lakh sms per month	-	17,000.00
113	Public IP	Additional public IP Addresses		1	-	150.00
114	DASHBOARDS	Network Monitoring dash Board		1	-	1,000.00
115	BACKUP Services	Backup agent , Backup management and monitoring , Back up Restoration		1	-	1,322.00
116	DATA TRANSFER	Bulk Data Transfer		1 TB	-	10,000.00
117		DATA SYNC service		1 TB	-	5,000.00
118	Developer Tools	Tools & SDKs or equivalent		1 instance	-	23,135.00
119		Code Deploy and commit tools or equivalent		1 instance	-	23,135.00
120	Mobile Services	Mobile Hub or equivalent		1	-	28,092.50
121		Mobile SDK		1	-	-
122		Container /Registry		1	-	4,627.00
123	Office 365(Email Service with 100 GB Mail Box each for primary and archival, Multiparty Video conferencing on PC, Laptop and tablets, personal data storage sync from PC to cloud, office productivity , search capabilities) or equivalent			1	-	-
Line Item #	SEC- F	Bare Metal Servers			HOURLY rate	MONTHLY rate
124	Intel Xeon E7-8890 v4 (192 Cores, 2.20 GHz),8192GB RAM (8192GB maximum), Up to 29 Internal Hard Drives Up to 10Gbps maximum Port Speeds, Redundant Power Supplies, Hypervisor Licenses, network connectivity to internet or Cloud infrastructure			1	-	1,174,281.89

125	Quad Intel Xeon E7-4890 v2 (60 Cores, 2.80 GHz) 2048GB RAM (2048GB maximum) Up to 24 Internal Hard Drives Up to 10Gbps maximum Port Speeds Redundant Power Supplies Hypervisor Licenses, network connectivity to internet or Cloud infrastructure			1	-	391,427.30
126	Intel Xeon E5-2690 v4, Dual Intel Xeon E5-2690 v4 (28 Cores, 2.60 GHz) 256GB RAM (256GB maximum) Up to 2 Internal Hard Drives Up to 10Gbps maximum Port Speeds Redundant Power Supplies Hypervisor Licenses, network connectivity to internet or Cloud infrastructure			1	-	88,071.14
Line Item #	Section G				HOURLY rate	MONTHLY rate
	Additional resources				-	-
127		1 Virtual CPU			-	500.00
128		1 GB RAM			-	50.00
129		Storage in minimum block of 50 GB			-	10.00
130		Additional network segment (per VLAN)			-	100.00
131		Additional 1 IP			-	125.00
132		Additional 1 sub-admin account			-	500.00
133	MSP Charges	5%				

Line Item #	Sec-A	Line Items			DC-Government Community Cloud 2 year		DR-Government Community Cloud 2 year		DC+DR-Government Community Cloud 2 year	
1	**VM**	**cpu**	**RAM**	**Storage (GB)**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**
2	Pack 1	1	1	50	14	9269.4	14.00	10,123.40	28.00	19,392.80
3	Pack 2	1	2	100	14	9562	15.40	10,389.40	29.40	19,951.40
4	Pack 3	2	4	100	22.4	16196.6	26.60	18,573.80	49.00	34,770.40
5	Pack 4	2	8	150	29.4	20434.4	28.00	20,102.60	57.40	40,537.00
6	Pack 5	2	16	150	29.4	20762	32.20	22,622.60	61.60	43,384.60
7	Pack 6	4	4	200	44.8	32313.4	51.80	37,077.60	96.60	69,391.00
8	Pack 7	4	8	250	44.8	32313.4	51.80	37,077.60	96.60	69,391.00
9	Pack 8	4	16	250	50.4	36054.2	50.40	35,949.20	100.80	72,003.40
10	Pack 9	6	6	300	88.2	63707	100.80	73,376.80	189.00	137,083.80
11	Pack 10	6	12	350	89.6	64428	102.20	74,030.60	191.80	138,458.60
12	Pack 11	8	8	400	89.6	64428	102.20	74,030.60	191.80	138,458.60
13	Pack 12	8	16	450	89.6	64428	102.20	74,030.60	191.80	138,458.60
14	Pack 13	8	32	450	99.4	71969.8	109.20	78,736.00	208.60	150,705.80

15	Pack 14	12	12	500	173.6	126520.8	200.20	145,930.40	373.80	272,451.20
16	Pack 15	12	24	550	175	126862.4	201.60	146,242.60	376.60	273,105.00
17	Pack 16	16	16	600	175	124275.2	244.80	146,508.60	457.30	270,783.80
18	Pack 17	16	32	650	175	127153.6	201.60	146,508.60	376.60	273,662.20
19	Pack 18	32	64	700	386.4	281729	424.20	309,362.20	810.60	591,091.20
20	Pack 19	64	128	750	770	561131.2	845.60	748,729.30	1,615.60	1,177,731.80
21	Pack 20	128	256	800	0	0	-	-	-	-
22	Bandwidth-Plan 1- upto 100 GB					754.00				
23	Bandwidth-Plan 2- upto 500 GB					3,927.00				
24	Bandwidth-Plan 3- upto 1000 GB					8,083.00				
25	Additional data transfer tariff per GB					8.00				

FOR CENTOS ONLY

Rates for other line items not available on centos

					Public Cloud											
					DC-Public Cloud 1 year		DR-Public Cloud 1 year		DC+DR-Public Cloud 1 year		DC-Public Cloud 2 year		DR-Public Cloud 2 year		DC+DR-Public Cloud 2 year	
Line Item #	**Sec-A**	**Line Items**			**Only for CentOS**		**Only for CentOS**		**Only for CentOS**		**Only for CentOS**		**Only for CentOS**		**Only for CentOS**	
	VM	cpu	RAM	Storage (GB)	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate
1	Pack 1	1	1	50	2.5	1800.0	2.3	1626.0	12.3	7355.0	2.5	1730.0	2.3	1550.0	12.3	7355.0
2	Pack 2	1	2	100	3.0	2160.0	2.7	1956.0	14.7	8810.0	3.0	2060.0	2.7	1850.0	14.7	8810.0
3	Pack 3	2	4	100	6.0	4320.0	5.4	3912.0	18.3	10970.0	6.0	4120.0	5.4	3700.0	18.3	10970.0
4	Pack 4	2	8	150	8.0	5760.0	7.2	5232.0	23.9	14315.0	8.0	5440.0	7.2	4900.0	23.9	14315.0
5	Pack 5	2	16	150	12.0	8640.0	10.8	7872.0	32.3	19355.0	12.0	8080.0	10.8	7300.0	32.3	19355.0
6	Pack 6	4	4	200	10.0	6760.0	9.0	6504.0	24.0	14420.0	10.0	6760.0	9.0	6200.0	24.0	14420.0
7	Pack 7	4	8	250	12.0	8370.0	10.8	7824.0	29.6	17765.0	12.0	8240.0	10.8	7400.0	29.6	17765.0
8	Pack 8	4	16	250	16.0	10890.0	14.4	10464.0	38.0	22805.0	16.0	10880.0	14.4	9800.0	38.0	22805.0
9	Pack 9	6	6	300	15.0	8990.0	13.5	9756.0	31.9	19130.0	15.0	8990.0	13.5	9300.0	31.9	19130.0
10	Pack 10	6	12	350	18.0	11230.0	16.2	11736.0	39.6	23735.0	18.0	11230.0	16.2	11100.0	39.6	23735.0
11	Pack 11	8	8	400	18.7	11220.0	18.0	12620.0	39.7	23840.0	18.7	11220.0	18.0	12400.0	39.7	23840.0
12	Pack 12	8	16	450	23.5	14090.0	21.6	15615.0	49.5	29705.0	23.5	14090.0	21.6	14800.0	49.5	29705.0
13	Pack 13	8	32	450	31.9	19130.0	28.8	20655.0	66.3	39785.0	31.9	19130.0	28.8	19600.0	66.3	39785.0
14	Pack 14	12	12	500	25.0	14980.0	27.0	16630.0	52.7	31610.0	25.0	14980.0	27.0	16630.0	52.7	31610.0
15	Pack 15	12	24	550	31.9	19110.0	32.4	20885.0	66.7	39995.0	31.9	19110.0	32.4	20885.0	66.7	39995.0
16	Pack 16	16	16	600	31.2	18740.0	34.4	20640.0	65.6	39380.0	31.2	18740.0	34.4	20640.0	65.6	39380.0
17	Pack 17	16	32	650	40.2	24130.0	43.2	26155.0	83.8	50285.0	40.2	24130.0	43.2	26155.0	83.8	50285.0
18	Pack 18	32	64	700	69.6	41760.0	73.2	43910.0	142.8	85670.0	69.6	41760.0	73.2	43910.0	142.8	85670.0
19	Pack 19	64	128	750	127.8	76670.0	131.6	78945.0	259.6	155615.0	127.8	76670.0	131.6	78945.0	259.6	155615.0

20	Pack 20	128	256	800	243.6	146140.0	247.6	148540.0	491.1	294680.0	243.6	146140.0	247.6	148540.0	491.1	294680.0
					VIRTUAL PRIVATE Cloud											
					DC-VIRTUAL Private Cloud 1 year		DR-VIRTUAL Private Cloud 1 year		DC+DR-VIRTUAL Private Cloud 1 year		DC-VIRTUAL Private Cloud 2 year		DR-VIRTUAL Private Cloud 2 year		DC+DR Virtual Private Cloud 1 year	
Line Item #	**Sec-A**	**Line Items**			**Only for CentOS**		**Only for CentOS**		**Only for CentOS**		**Only for CentOS**		**Only for CentOS**		**Only for CentOS**	
	VM	cpu	RAM	Storage (GB)	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**
1	Pack 1	1	1	50	8.70	5200.00	10.00	5725.00	18.21	10925.00	8.70	5200.00	10.00	5725.00	18.21	10925
2	Pack 2	1	2	100	10.00	6050.00	10.00	6700.00	21.00	12750.00	10.00	6050.00	10.00	6700.00	21	12750
3	Pack 3	2	4	100	12.30	7400.00	13.00	8050.00	25.75	15450.00	12.30	7400.00	13.00	8050.00	25.75	15450
4	Pack 4	2	8	150	15.80	9450.00	17.00	10225.00	32.79	19675.00	15.80	9450.00	17.00	10225.00	32.79	19675
5	Pack 5	2	16	150	21.00	12650.00	21.00	13425.00	43.46	26075.00	21.00	12650.00	21.00	13425.00	43.46	26075
6	Pack 6	4	4	200	15.70	9400.00	17.00	10300.00	32.83	19700.00	15.70	9400.00	17.00	10300.00	32.83	19700
7	Pack 7	4	8	250	19.10	11450.00	21.00	12475.00	39.88	23925.00	19.10	11450.00	21.00	12475.00	39.88	23925
8	Pack 8	4	16	250	24.40	14650.00	26.00	15675.00	50.54	30325.00	24.40	14650.00	26.00	15675.00	50.54	30325
9	Pack 9	6	6	300	20.30	12200.00	22.00	13350.00	42.58	25550.00	20.30	12200.00	22.00	13350.00	42.58	25550
10	Pack 10	6	12	350	25.10	15050.00	27.00	16325.00	52.29	31375.00	25.10	15050.00	27.00	16325.00	52.29	31375
11	Pack 11	8	8	400	25.00	15000.00	27.00	16400.00	52.33	31400.00	25.00	15000.00	27.00	16400.00	52.33	31400
12	Pack 12	8	16	450	31.10	18650.00	34.00	20175.00	64.71	38825.00	31.10	18650.00	34.00	20175.00	64.71	38825
13	Pack 13	8	32	450	41.80	25050.00	44.00	26575.00	86.04	51624.00	41.80	25050.00	44.00	26575.00	86.04	51624
14	Pack 14	12	12	500	32.80	19700.00	36.00	21350.00	68.42	41050.00	32.80	19700.00	36.00	21350.00	68.42	41050
15	Pack 15	12	24	550	46.10	24950.00	45.00	26725.00	86.13	51675.00	46.10	24950.00	45.00	26725.00	86.13	51675
16	Pack 16	16	16	600	40.70	24400.00	44.00	26300.00	84.50	50700.00	40.70	24400.00	44.00	26300.00	84.5	50700
17	Pack 17	16	32	650	52.10	31250.00	55.00	33275.00	107.54	64525.00	52.10	31250.00	55.00	33275.00	107.54	64525
18	Pack 18	32	64	700	88.80	53300.00	92.00	55450.00	181.25	108750.00	88.80	53300.00	92.00	55450.00	181.25	108750
19	Pack 19	64	128	750	161.60	96950.00	165.00	99225.00	326.96	196175.00	161.60	96950.00	165.00	99225.00	326.96	196175
20	Pack 20	128	256	800	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0	0
					Government Community Cloud											
					DC-GCC 1 year		DR-GCC 1 year		DC+DR-GCC 1 year		DC-GCC 2 year		DR-GCC 2 year		DC+DR-GCC 2 year	
Line Item #	**Sec-A**	**Line Items**			**Only for CentOS**		**Only for CentOS**		**Only for CentOS**		**Only for CentOS**		**Only for CentOS**		**Only for CentOS**	
	VM	cpu	RAM	Storage (GB)	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**	**HOURLY rate**	**MONTHLY rate**
1	Pack 1	1	1	50	12.30	7,375.00	13.00	7,950.00	25.54	15,325.00	12.3	7375	13.00	7,950.00	25.54	15,325.00
2	Pack 2	1	2	100	14.00	8,500.00	15.00	9,250.00	29.40	17,750.00	14	8500	15.00	9,250.00	29.40	17,750.00

3	Pack 3	2	4	100	17.10	10,250.00	19.00	11,100.00	35.58	21,350.00	17.1	10250	19.00	11,100.00	35.58	21,350.00
4	Pack 4	2	8	150	21.50	12,875.00	23.00	14,050.00	44.88	26,925.00	21.5	12875	23.00	14,050.00	44.88	26,925.00
5	Pack 5	2	16	150	28.10	16,875.00	31.00	18,450.00	58.88	35,325.00	28.1	16875	31.00	18,450.00	58.88	35,325.00
6	Pack 6	4	4	200	21.70	13,000.00	24.00	14,100.00	45.17	27,100.00	21.7	13000	24.00	14,100.00	45.17	27,100.00
7	Pack 7	4	8	250	26.00	15,625.00	28.00	17,050.00	54.46	32,675.00	26	15625	28.00	17,050.00	54.46	32,675.00
8	Pack 8	4	16	250	32.70	19,625.00	36.00	21,450.00	68.46	41,075.00	32.7	19625	36.00	21,450.00	68.46	41,075.00
9	Pack 9	6	6	300	27.90	16,750.00	30.00	18,200.00	58.25	34,950.00	27.9	16750	30.00	18,200.00	58.25	34,950.00
10	Pack 10	6	12	350	34.00	20,375.00	37.00	22,250.00	71.04	42,625.00	34	20375	37.00	22,250.00	71.04	42,625.00
11	Pack 11	8	8	400	34.20	20,500.00	37.00	22,300.00	71.33	42,800.00	34.2	20500	37.00	22,300.00	71.33	42,800.00
12	Pack 12	8	16	450	41.90	25,125.00	46.00	27,450.00	87.63	52,575.00	41.9	25125	46.00	27,450.00	87.63	52,575.00
13	Pack 13	8	32	450	55.20	33,125.00	60.00	36,250.00	115.63	69,375.00	55.2	33125	60.00	36,250.00	115.63	69,375.00
14	Pack 14	12	12	500	44.60	26,750.00	48.00	29,000.00	92.92	55,750.00	44.6	26750	48.00	29,000.00	92.92	55,750.00
15	Pack 15	12	24	550	55.60	33,375.00	61.00	36,300.00	116.21	69,725.00	55.6	33375	61.00	36,300.00	116.21	69,725.00
16	Pack 16	16	16	600	55.00	33,000.00	60.00	35,700.00	114.50	68,700.00	55	33000	60.00	35,700.00	114.50	68,700.00
17	Pack 17	16	32	650	69.40	41,625.00	75.00	45,250.00	144.79	86,875.00	69.4	41625	75.00	45,250.00	144.79	86,875.00
18	Pack 18	32	64	700	117.10	70,250.00	126.00	75,600.00	243.08	145,850.00	117.1	70250	126.00	75,600.00	243.08	145,850.00
19	Pack 19	64	128	750	211.50	126,875.00	226.00	135,550.00	437.38	262,425.00	211.5	126875	226.00	135,550.00	437.38	262,425.00
20	Pack 20	128	256	800	399.20	239,500.00	425.00	254,700.00	823.67	494,200.00	399.2	239500	425.00	254,700.00	823.67	494,200.00

Tier 2 Empanelment rate

Public Cloud

					Public Cloud						**Virtual Private Cloud**						**Government Community Cloud**					
Line Item #	**Sec-A**	**Line Items**			DC-Public Cloud 1 year		DR-Public Cloud 1 year		DC+DR-Public Cloud 1 year		DC-Virtual Private Cloud 1 year		DR-Virtual Private Cloud 1 year		DC+DR-Virtual Private Cloud 1 year		DC-GCC 1 year		DR-GCC 1 year		DC+DR-GCC 1 year	
	VM	cpu	RAM	Storage	HOURLY	MONTH	HOURLY	MONTH	HOURLY	MONTH	HOURLY	MONTH	HOURLY	MONTH	HOURLY	MONTH	HOURLY	MONTH	HOURLY	MONTH	HOURLY	MONTH

				(GB)	rate	LY rate	rate	LY rate	rate	LY rate	rate	LY rate	rate	LY rate	rate	LY rate	rate	LY rate	rate	LY rate	rate	LY rate	rate	LY rate
1	Pack 1	1	1	50	8.19	5,900	8.19	5900.00	8.19	5900.00	8.2	5900.0	8.2	5900.0	8.2	5900.0	8.2	5900.0	8.2	5900.0	8.2	5900.0	8.2	5900.0
2	Pack 2	1	2	100	8.54	6,150	8.54	6150.00	8.54	6150.00	8.5	6150.0	8.5	6150.0	8.5	6150.0	8.5	6150.0	8.5	6150.0	8.5	6150.0	8.5	6150.0
3	Pack 3	2	4	100	8.96	6,450	8.96	6450.00	8.96	6450.00	9.0	6450.0	9.0	6450.0	9.0	6450.0	9.0	6450.0	9.0	6450.0	9.0	6450.0	9.0	6450.0
4	Pack 4	2	8	150	9.72	7,000	9.72	7000.00	9.72	7000.00	9.7	7000.0	9.7	7000.0	9.7	7000.0	9.7	7000.0	9.7	7000.0	9.7	7000.0	9.7	7000.0
5	Pack 5	2	16	150	10.83	7,800	10.83	7800.00	10.83	7800.00	10.8	7800.0	10.8	7800.0	10.8	7800.0	10.8	7800.0	10.8	7800.0	10.8	7800.0	10.8	7800.0
6	Pack 6	4	4	200	10.35	7,450	10.35	7450.00	10.35	7450.00	10.4	7450.0	10.4	7450.0	10.4	7450.0	10.4	7450.0	10.4	7450.0	10.4	7450.0	10.4	7450.0
7	Pack 7	4	8	250	11.11	8,000	11.11	8000.00	11.11	8000.00	11.1	8000.0	11.1	8000.0	11.1	8000.0	11.1	8000.0	11.1	8000.0	11.1	8000.0	11.1	8000.0
8	Pack 8	4	16	250	12.22	8,800	12.22	8800.00	12.22	8800.00	12.2	8800.0	12.2	8800.0	12.2	8800.0	12.2	8800.0	12.2	8800.0	12.2	8800.0	12.2	8800.0
9	Pack 9	6	6	300	14.1	10,150	14.10	10150.00	14.10	10150.00	14.1	10150.0	14.1	10150.0	14.1	10150.0	14.1	10150.0	14.1	10150.0	14.1	10150.0	14.1	10150.0
10	Pack 10	6	12	350	15.14	10,900	15.14	10900.00	15.14	10900.00	15.1	10900.0	15.1	10900.0	15.1	10900.0	15.1	10900.0	15.1	10900.0	15.1	10900.0	15.1	10900.0
11	Pack 11	8	8	400	16.11	11,600	16.11	11600.00	16.11	11600.00	16.1	11600.0	16.1	11600.0	16.1	11600.0	16.1	11600.0	16.1	11600.0	16.1	11600.0	16.1	11600.0
12	Pack 12	8	16	450	17.64	12,700	17.64	12700.00	17.64	12700.00	17.6	12700.0	17.6	12700.0	17.6	12700.0	17.6	12700.0	17.6	12700.0	17.6	12700.0	17.6	12700.0
13	Pack 13	8	32	450	20.42	14,700	20.42	14700.00	20.42	14700.00	20.4	14700.0	20.4	14700.0	20.4	14700.0	20.4	14700.0	20.4	14700.0	20.4	14700.0	20.4	14700.0
14	Pack 14	12	12	500	17.78	12,800	17.78	12800.00	17.78	12800.00	17.8	12800.0	17.8	12800.0	17.8	12800.0	17.8	12800.0	17.8	12800.0	17.8	12800.0	17.8	12800.0
15	Pack 15	12	24	550	20	14,400	20.00	14400.00	20.00	14400.00	20.0	14400.0	20.0	14400.0	20.0	14400.0	20.0	14400.0	20.0	14400.0	20.0	14400.0	20.0	14400.0
16	Pack 16	16	16	600	19.44	14,000	19.44	14000.00	19.44	14000.00	19.4	14000.0	19.4	14000.0	19.4	14000.0	19.4	14000.0	19.4	14000.0	19.4	14000.0	19.4	14000.0
17	Pack 17	16	32	650	22.36	16,100	22.36	16100.00	22.36	16100.00	22.4	16100.0	22.4	16100.0	22.4	16100.0	22.4	16100.0	22.4	16100.0	22.4	16100.0	22.4	16100.0
18	Pack 18	32	64	700	55.16	39,713	55.16	39713.00	55.16	39713.00	55.2	39713.0	55.2	39713.0	55.2	39713.0	55.2	39713.0	55.2	39713.0	55.2	39713.0	55.2	39713.0
19	Pack 19	64	128	750	88.63	63,813	88.63	63813.00	88.63	63813.00	88.6	63813.0	88.6	63813.0	88.6	63813.0	88.6	63813.0	88.6	63813.0	88.6	63813.0	88.6	63813.0
20	Pack 20	128	256	800	155.43	111,913	155.43	111913.00	155.43	111913.00	155.4	111913.0	155.4	111913.0	155.4	111913.0	155.4	111913.0	155.4	111913.0	155.4	111913.0	155.4	111913.0
21	Bandwidth-Plan 1-upto 100 GB	800																						
22	Bandwidth-Plan 2-upto 500 GB	4000																						
23	Bandwidth-Plan 3-upto 1000 GB	8000																						
24	Additional data transfer tariff per GB	8																						

Line Item #	SEC- B STORAGE	Line Items		MONTHLY rate	Line Item #	SEC-C DATABASE	Database Options	No. of Licenses required	MONTHLY rate
25	Object storage	50 GB		100	61	Postgre Enterprise		4	3,412.00
26		500 GB		1000	62			5 to 8	3,412.00
27		1000 GB		2000	63			> 8	3,412.00

28		10 TB		16000	64	MySQL 4 socket, 8 socket, 16 socket and 32 socket	4 socket	
29	File storage	50 GB		125	65		8 socket	
30		500 GB		1250	66		16 socket	
31		1000 GB		2500	67		32 socket	
32		10 TB		20000	68	MySQL Standard	4	6,489.00
33	Archive storage	50 GB		75	69		5 to 8	5,948.00
34		500 GB		750	70		> 8	5,408.00
35		1000 GB		1500	71	MySQL Enterprise	4	16,222.00
36		10 TB		12000	72		5 to 8	14,871.00
37	DISK storage	50 GB	<= 120 IOPS	100	73		> 8	13,519.00
38			121 to 400 IOPS	100	74	MSSQL 2012 Standard	4	7,000.00
39			401 to 800 IOPS	100	75		5 to 8	7,000.00
40			801 to 1200 IOPS	100	76		> 8	7,000.00
41			1201 to 2000 IOPS	300	77	MSSQL 2012 Enterprise	4	27,000.00
42			> 5000 IOPS	300	78		5 to 8	27,000.00
43		500 GB	<= 120 IOPS	1000	79		> 8	27,000.00
44			121 to 400 IOPS	1000	80	Oracle Standard	4	18,168.00
45			401 to 800 IOPS	1000	81		5 to 8	18,168.00
46			801 to 1200 IOPS	1000	82		> 8	18,168.00
47			1201 to 2000 IOPS	3000	83	Oracle Enterprise	4	27,043.00
48			> 5000 IOPS	3000	84		5 to 8	27,043.00
49		1000 GB	<= 120 IOPS	2000	85		> 8	27,043.00
50			121 to 400 IOPS	2000	86	NoSQL Enterprise	100	11,969.00
51			401 to 800 IOPS	2000	87		101 to 500	11,969.00
52			801 to 1200 IOPS	2000	88		501 to 1000	23,937.00
53			1201 to 2000 IOPS	6000	89		> 1000	47,874.00
54			> 5000 IOPS	6000	90	IBM DB2 v 10.5 or above	2	99,400.00
55		10 TB	<= 120 IOPS	16000	91		4	99,400.00
56			121 to 400 IOPS	16000	92		10	99,400.00
57			401 to 800 IOPS	16000	93		> 10	99,400.00
58			801 to 1200 IOPS	16000	94	NoSQL DB	100	11,969.00
59			1201 to 2000 IOPS	48000	95		101 to 500	11,969.00
60			> 5000 IOPS	48000	96		501 to 1000	23,937.00
					97		> 1000	47,874.00
					98	MySQL & Postgre SQL compatible relational database	4	6,489.00
					99		5 to 8	5,948.00
					100		> 8	5,408.00

Line Item #	SEC-E SERVICES			Price per Unit per Month if services taken for 1 year		Price per Unit per Month if services taken for 2 years
105	Scalability	Virtual Machine Scale Sets/Auto Scaling	1 unit of 5 VMs	10		10
106	DNS	DNS Management	1	75		75
		price quoted is for per DNS entry				
107	AD	Active Directory Services price quoted is for per User.	1	25		25
108	VPN	VPN / Gateway	2 ports per VPN	300		300

		SITE to SITE Point to Point				
109	API	API Gateway/ Management	1	15,000		15,000
110		Email gateway				
	Email/SMS	prices quoted are for open source email solution	1 account with 10 GB	70		70
111		SMS gateway	1 lakh sms per month	11,000		11,000
112		Additional public IP Addresses	1	300		300
113	DASHBOARDS	Network Monitoring dash Board (Per Device/instance)	1	300		300
114		Backup agent	1	500		500
	BACKUP Services	Backup management and monitoring	1	1,000		2,000
		Back up Restoration	1	1,000		1,000
115		Bulk Data Transfer	1 TB	3,000		3,000
116	DATA TRANSFER	DATA SYNC service				
		Prices quoted are for data sync between ESDS Data centers.	1 TB	2,500		2,500
117	Developer Tools	Tools & SDKs or equivalent	1 instance	51,000		51,000
		Code Deploy and commit tools or equivalent	1 instance	51,000		51,000
118		Mobile Hub or equivalent	1	11,000		11,000
119	Mobile Services	Mobile SDK	1	11,000		11,000
120		Container /Registry	1	51,000		51,000
121	Office 365(Email Service with 100 GB Mail Box for primary and archival, Multiparty Video conferencing on PC, Laptop and tablets, personal data storage sync from PC to cloud, office productivity , search capabilities) or equivalent		1	-		-

Line Item #	SEC- F- Bare Metal Servers		RateperMonth perUnit (Rs)if servicestaken for1year	RateperMonthper Unit (Rs)if services takenfor2year
122	Intel Xeon E7-8890 v4 (192 Cores, 2.20 GHz),8192GB RAM (8192GB maximum), Up to 29 Internal Hard Drives Up to 10Gbps maximum Port Speeds, Redundant Power Supplies, Hypervisor Licenses, network connectivity to internet or Cloud infrastructure	1	537,389	510,520
123	Quad Intel Xeon E7-4890 v2 (60 Cores, 2.80 GHz) 2048GB RAM (2048GB maximum) Up to 24 Internal Hard Drives Up to 10Gbps maximum Port Speeds Redundant Power Supplies Hypervisor Licenses, network connectivity to internet or Cloud infrastructure	1	142,271	135,158
124	Intel Xeon E5-2690 v4, Dual Intel Xeon E5-2690 v4 (28 Cores, 2.60 GHz) 256GB RAM (256GB maximum) Up to 2 Internal Hard Drives Up to 10Gbps maximum Port Speeds Redundant Power Supplies Hypervisor Licenses, network connectivity to internet or Cloud infrastructure	1	41,654	39,571

Line Item #	Section G	Additional resources	MONTHLY rate per GB
125	1 Virtual CPU		450.00
126	1 GB RAM		220.00
127	Storage in minimum block of 50 GB		243.00
128	Additional network segment (per VLAN)		-
129	Additional 1 IP		100.00
130	Additional 1 sub-admin account		500.00
131	MSP Charges		5%

Government Circular No.: **मातंसं - 060/3/2017/1**

					Public Cloud						Virtual Private Cloud						Government Community Cloud					
Line Item #	**Sec-A**	**Line Items**			DC-Public Cloud 2 year		DR-Public Cloud 2 year		DC+DR-Public Cloud 2 year		DC-Virtual Private Cloud 2 year		DR-Virtual Private Cloud 2 year		DC+DR-Virtual Private Cloud 2 year		DC-GCC 2 year		DR-GCC 2 year		DC+DR-GCC 2 year	
	VM	cpu	RAM	Storage (GB)	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate	HOURLY rate	MONTHLY rate
1	Pack 1	1	1	50	8.19	5,900	8.19	5900.00	8.19	5900.00	8.2	5900.0	8.2	5900.0	8.2	5900.0	8.2	5900.0	8.2	5900.0	8.2	5900.0
2	Pack 2	1	2	100	8.54	6,150	8.54	6150.00	8.54	6150.00	8.5	6150.0	8.5	6150.0	8.5	6150.0	8.5	6150.0	8.5	6150.0	8.5	6150.0
3	Pack 3	2	4	100	8.96	6,450	8.96	6450.00	8.96	6450.00	9.0	6450.0	9.0	6450.0	9.0	6450.0	9.0	6450.0	9.0	6450.0	9.0	6450.0
4	Pack 4	2	8	150	9.72	7,000	9.72	7000.00	9.72	7000.00	9.7	7000.0	9.7	7000.0	9.7	7000.0	9.7	7000.0	9.7	7000.0	9.7	7000.0
5	Pack 5	2	16	150	10.83	7,800	10.83	7800.00	10.83	7800.00	10.8	7800.0	10.8	7800.0	10.8	7800.0	10.8	7800.0	10.8	7800.0	10.8	7800.0
6	Pack 6	4	4	200	10.35	7,450	10.35	7450.00	10.35	7450.00	10.4	7450.0	10.4	7450.0	10.4	7450.0	10.4	7450.0	10.4	7450.0	10.4	7450.0
7	Pack 7	4	8	250	11.11	8,000	11.11	8000.00	11.11	8000.00	11.1	8000.0	11.1	8000.0	11.1	8000.0	11.1	8000.0	11.1	8000.0	11.1	8000.0
8	Pack 8	4	16	250	12.22	8,800	12.22	8800.00	12.22	8800.00	12.2	8800.0	12.2	8800.0	12.2	8800.0	12.2	8800.0	12.2	8800.0	12.2	8800.0
9	Pack 9	6	6	300	14.1	10,150	14.10	10150.00	14.10	10150.00	14.1	10150.0	14.1	10150.0	14.1	10150.0	14.1	10150.0	14.1	10150.0	14.1	10150.0
10	Pack 10	6	12	350	15.14	10,900	15.14	10900.00	15.14	10900.00	15.1	10900.0	15.1	10900.0	15.1	10900.0	15.1	10900.0	15.1	10900.0	15.1	10900.0
11	Pack 11	8	8	400	16.11	11,600	16.11	11600.00	16.11	11600.00	16.1	11600.0	16.1	11600.0	16.1	11600.0	16.1	11600.0	16.1	11600.0	16.1	11600.0
12	Pack 12	8	16	450	17.64	12,700	17.64	12700.00	17.64	12700.00	17.6	12700.0	17.6	12700.0	17.6	12700.0	17.6	12700.0	17.6	12700.0	17.6	12700.0
13	Pack 13	8	32	450	20.42	14,700	20.42	14700.00	20.42	14700.00	20.4	14700.0	20.4	14700.0	20.4	14700.0	20.4	14700.0	20.4	14700.0	20.4	14700.0
14	Pack 14	12	12	500	17.78	12,800	17.78	12800.00	17.78	12800.00	17.8	12800.0	17.8	12800.0	17.8	12800.0	17.8	12800.0	17.8	12800.0	17.8	12800.0
15	Pack 15	12	24	550	20	14,400	20.00	14400.00	20.00	14400.00	20.0	14400.0	20.0	14400.0	20.0	14400.0	20.0	14400.0	20.0	14400.0	20.0	14400.0
16	Pack 16	16	16	600	19.44	14,000	19.44	14000.00	19.44	14000.00	19.4	14000.0	19.4	14000.0	19.4	14000.0	19.4	14000.0	19.4	14000.0	19.4	14000.0
17	Pack 17	16	32	650	22.36	16,100	22.36	16100.00	22.36	16100.00	22.4	16100.0	22.4	16100.0	22.4	16100.0	22.4	16100.0	22.4	16100.0	22.4	16100.0
18	Pack 18	32	64	700	55.16	39,713	55.16	39713.00	55.16	39713.00	55.2	39713.0	55.2	39713.0	55.2	39713.0	55.2	39713.0	55.2	39713.0	55.2	39713.0
19	Pack 19	64	128	750	88.63	63,813	88.63	63813.00	88.63	63813.00	88.6	63813.0	88.6	63813.0	88.6	63813.0	88.6	63813.0	88.6	63813.0	88.6	63813.0
20	Pack 20	128	256	800	155.43	111,913	155.43	111913.00	155.43	111913.00	155.4	111913.0	155.4	111913.0	155.4	111913.0	155.4	111913.0	155.4	111913.0	155.4	111913.0
21	Bandwidth-Plan 1-upto 100 GB				800																	
22	Bandwidth-Plan 2-upto 500 GB				4000																	
23	Bandwidth-Plan 3-upto 1000 GB				8000																	
24	Additional data transfer tariff per GB				8																	

****

Annexure 2

SCOPE OF WORK
&
Standard Operating Procedure

For availing Hosting and Cloud Services from Empanelled Cloud Service Providers for Government of Maharashtra

Directorate of Information Technology Government of Maharashtra

GAD-060/3/2017/2

Issued By: -
Directorate of Information Technology,
7th Floor, Annex Building
Mantralaya, Mumbai – 400032
Tel: 022 - 22044586

Introduction

Considering the growing adoption of online services by citizens of the State & use of IT Within Government, there is a constantly increasing demand from Departments for infrastructure for hosting services including disaster recovery and backup for their various IT applications.

Government of Maharashtra has formulated the Cloud Computing Policy of the State. (Available on www.maharashtra.gov.in) This policy has come into force from 29.01.2018. As per this policy, all Government organizations must use cloud infrastructure services instead of using Government owned data centers or data centers owned by the organization or co-locating their infrastructure in any Government owned/ privately owned data center. DIT has been empanel cloud service providers from whom Departments can avail of cloud services.

The scope of empanelment is as follows:

1. Empanelling CSPs for providing cloud service offerings to end user departments from specified data centers for a period of **3 years**.
2. Discovering the unit rates for the cloud service offerings which has been apply for a period of **2 years**. After a period of 2 years, empanelled CSPs has been be asked to submit revised rates.

1 Performance Bank Guarantee

The Performance Bank Guarantee to be furnished by the empanelled CSP to DIT (hereinafter referred to as "PBG") is for an amount of Rs. 50 Lac. PBG amount will be refunded after completion of the contract period (3 years). PBG would be discharged/ returned by DIT upon being satisfied that there has been due performance of the obligations of the CSP/MSP under the contract at the end of the contract.

In addition to this, for work order value exceeding Rs. 5 lakhs in a financial year, the empanelled CSP to deposit a PBG of 10 % of the contract value with the respective user Department within 15 days of issue of work order.

In the event of the CSP/MSP being unable to service the contract for whatever reason DIT would forfeit the PBG. Notwithstanding and without prejudice to any rights whatsoever of DIT under the contract in the matter, the proceeds of the PBG shall be payable to DIT as compensation for any loss resulting from the CSP/MSPs failure to complete its obligations under the Contract. DIT shall notify the CSP/MSP in writing of the exercise of its right to receive such compensation within 14 days, indicating the contractual obligation(s) for which the CSP/MSP is in default.

DIT shall also be entitled to make recoveries from the CSP/MSP's bills, PBG, or from any other amount due to him, the equivalent value of any payment made to him due to inadvertence, error, collusion, and misstatement.

Key Considerations for Cloud Procurement

S.No	Considerations	Conventional IT Projects	Cloud Service Project
1.	Requirements Estimation (compute, storage, memory, software licenses..,)	The Department needs to estimate the requirements for the total duration of the project (forecasting for 3 or 5 years) and indicates the BoM based on the assessed requirements in the RFP	For Cloud Procurement, the Department may not undertake the estimation for the entire project duration. The Minimum / Indicative Day One requirements can be indicated in the SCOPE of WORK to be circulated to empaneled CSPs
2.	Flexibility to Procure Variable Quantity of the Same Service	For a conventional Project, if the Department has any additional procurement requirements(servers, storage,) it has to go through the procurement process	The flexibility to scale up/down and the ability to provision virtual machines, storage and bandwidth dynamically enable procurement of additional requirements hassle free.
3.	Scenario Based Pricing	Since the requirements for the entire duration of project need to be specified in the RFP, the pricing becomes a Fixed Price model	For cloud procurement two plausible pricing options are possible: #1- Indicative requirements #2 Minimum Requirements with indicative Peak Load
4.	Payment Model	As a corollary to the requirements and Pricing model, the Payment terms are fixed timelines based payments	With the option of scaling up or down based on the requirements, procurement of cloud services is Pay-As-You-Go utility model
5.	Shared Responsibility	The Responsibility of the Project and deliverables lies with Selected bidder.	The responsibility of the Project, (owing to critical Security concerns) is shared between the CSP and the Department.
6.	Standardized SLA	The conventional IT projects have largely well-defined and accepted SLAs across the Project domains.	SLAs critical to cloud services need to be identified and to be incorporated in the project agreement As defined in section 4 of this document
7.	Contractual Clauses	Traditional IT projects have fairly standardized contracts.	Contractual clauses Specific to Cloud need to be addressed in the SOW (Legal Compliance, Exit Management, payment terms...)

SECTION 2

Scope of empanelment

DIT is empanelling cloud service providers offering the following cloud services for empanelment of their cloud service offerings for a combination of the Deployment Models (Public Cloud, Virtual Private Cloud and Government Community Cloud).

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Disaster Recovery as a Service (DRaaS)

The Government Departments & agencies will select the appropriate cloud service offerings based on the risk & security profile of their applications / data / services using guidelines issued by DIT from time to time.

2.1 Requirements

The requirements for various cloud offerings including IaaS, PaaS and DRaaS offerings and various deployment models- public cloud, virtual private cloud and Government Community Cloud. In future, DIT may expand this list following a process similar to this empanelment.

As per the cloud policy of the State, a majority of these resources are expected to shift to the empanelled CSPs by 30th October 2018. Therefore, in order to create a fast, flexible process that capitalizes on the full scale and flexibility of the cloud, Departments may consider the following key components while procuring Cloud Services.

1 Cloud Services Requirements
2 Security – Shared Responsibility
3 Migration of Existing Systems to Cloud
4 Operational & Monitoring Requirements
5 Exit Management/Transitioning out services
6 Managed Services
7 Role of Government Departments
8 Pay-As-You-Go
9 Contractual Terms and Service Level Objectives

Migration to Cloud document can be referred to for migrating the applications to cloud of Empanelled CSPs.

2.2 Operational acceptance from Department

For User Department while getting on boarded onto cloud with support from the MSP, if required, Operational Acceptance shall commence once the system is commissioned for a period of 30 days.

Operational Acceptance will be provided by the Department after cloud resources have been provisioned and switchover testing (as applicable) has been completed. Switchover testing would include:

i. Switch over of application from DC to DR as per defined RTO and RPO
ii. Switch over applications from DR to DC as predefined RTO and RPO
iii. Complete Data Replication and Reverse Data Replication as per RPO
iv. Fully functional application while DR site is operational, taking into consideration the end user experience

In case only DC or DR services have been requested, then operational acceptance will not involve switchover testing.

2.3 **Audit by DIT**

DIT will also ensure that third party audit of empanelled Cloud service providers (CSP) is carried out at least once a year.

2.4 Helpdesk Support

Each empanelled CSP is required to create and maintain a Help Desk / telephonic number and email based ticketing system that will resolve problems and answer queries related to DC/DR site. The help desk support to users shall be provided on 24x7x365 basis over telephone, chat and ticketing system.

SECTION 3
Pricing

3.1 Pricing model

Rates discovered through CSP empanelment RFP for a set of options which Departments can use are exclusive of taxes. GST will be applicable as per prevailing rates on the date of issue of raising the invoices.

The L1 (lowest) rates for each line item are being notified with a list of technically qualified bidders who have agreed to match the L1 rates and the L1 rates for the particular line item. The notified rates will be valid for a period of 2 years from the date of notification.

3.2 Free trial

To ensure that Departments get a hands on experience before they choose the CSP, all the empanelled CSPs will be required to provide Departments with the facility of a free trial for a limited period of 30 days whereby users can experience the various cloud offerings before the Department decides to select their CSP.

3.3 Payments linked to utilization

In the case of virtual machines provisioned by user Departments, the billing for cloud services will be be based on actual consumption of services (Pay-As-You-Go model) with zero capital (one time) cost.

To incentivize optimal solution design and encourage proper utilization of the assigned computing resources, empanelled CSP in co-ordination with the user Department should ensure that the average monthly utilization of RAM, CPU and storage is not less than 50%.

If the average monthly utilization is less than 50% in a particular month, the CSP should immediately notify the user Department. The user Department and the MSP/CSP should undertake a joint assessment within 15 days, analyze the reasons for the utilization being less than 50% and undertake steps to ensure resource utilization of at least 50%.

If the average monthly utilization of RAM or CPU or storage is less than 50% for 2 successive months, a penalty of 25% of the monthly bill amount (from the next billing cycle) will apply for those particular months where utilization is below 50%.

However, if the CSP has proposed a resource optimization plan to bring the average utilization above 50% but such plan has not been approved by the user Department within the above time period of 2 months, the penalty will be waived off by DIT.

If average monthly utilization exceeds 65%, an additional incentive of 5% of the monthly bill amount has been be payable to the CSP for a period not exceeding 6 months.
The expenditure towards cloud services has been be borne by the user Department from their budgetary resources. It is clarified that DIT has been not bear the expenditure centrally for availing cloud services.

Empanelled Cloud Service providers should raise quarterly invoices to the respective Department. Payments will be ordinarily made by the respective user Department within 1 month of the raising of the invoice.

SECTION 4
Service level norms

4.1 Service level norms and Service level agreement

a) Individual user Departments will enter into service level agreements related to implementation (where Department avails of managed services) with the empanelled CSP. DIT has been circulate sample templates for the same.

b) The service level norms for provision of cloud service offerings will be as per the MeiTY document "Guidelines for Government Departments On Service Level Agreement For Procuring Cloud Services" published by MeitY on 31st March 2017. These guidelines are available at http://meity.gov.in/writereaddata/files/Guidelines-Service_Levels.pdf. In addition to this, DIT reserves the right to lay down service level norms for any activities not mentioned in the above document.

c) In case the mandated service levels are not achieved, the user Department shall invoke the performance related penalties. Payments to the CSP has been linked to the compliance with the SLA metrics. To illustrate calculation of penalties, an indicative example is provided below.

- The payment should be linked to the compliance with the SLA metrics.
- The penalty in percentage of the monthly payment has been be as indicated against each SLA parameter in the table.

For ex: For SLA1 if the penalty to be levied is 7% then 7% of the Quarterly Payment is deducted from the total of the Quarterly bill and the balance paid to the CSP.
If the penalties are to be levied in more than one SLA then the total applicable penalties are calculated and deducted from the total of the Quarterly bill and the balance paid to the CSP.

For ex: SLA1 =7% of the Quarterly Payment, SLA12=10% of the Quarterly Payment, SLA19=2% of the Quarterly Payment then,

Amount to be paid = Total Quarterly bill – {(19% of the Quarterly Payment)}

SECTION 5
Activities to be performed by MSP

5.1 System Planning:

The MSP should submit a detailed plan regarding cloud deployment and configuration to the Department. This plan should include the following

a. CPU, RAM, Storage requirement
b. On line and full off line backup of existing system Notification of downtime to end users
c. System export window
d. Replication tool configuration
e. Transfer time of data from DC to DR Data restoration at DR side.
f. Data Sync times and dependencies if any Switching on DC servers
g. Notifying end users.
h. Coordination with other vendors
i. Network architecture planning including VLAN configuration planning, IP address planning & Subnet planning and routing planning Firewall configuration planning
j. Backup methodology
k. Failover mechanism for replication links Business continuity Architecture planning

On acceptance of the above plan by the user Department, the MSP should assist the Department in deploying/migrating the Departmental application onto the cloud and offer for testing.

5.2 Testing:

Following cloud resource deployment/provisioning, the MSP must perform following testing:

a. **Functional Testing**: Once system is exported, data is migrated to Cloud site and application started functioning, the functional testing of Application will be done by the user Department Team along with application vendors. The MSP requires to provide support and co-ordination in this case.
b. Department and application developers/system integrators may perform following testing.
    i. Software Module testing as per functional requirement.
    ii. User authentications testing.
    iii. Users add/delete, reports generations
    iv. Heavy application transactions on DR servers
    v. Data upload/Download
    vi. Connection per second /user per second
    vii. Backup exports
    viii. Backup restoration
    ix. SMS/Email Gateway Integeration/testing
    x. API integration with other applications if required
    xi. Payment gateway integration

c. **Data Integrity Testing**: Data integrity testing will be performed by Department staff and application vendors which would include:
    i. Amount of data verification at both end
    ii. Table size and records testing.
    iii. User status at both ends.
    iv. Invoices/transactions verification at both ends.
    v. Data in log files.

d. **Business Continuity Testing:** In the event of a disaster at DC site, activation of services from the DR site is the responsibility of MSP. The MSP shall develop appropriate policy, checklists in line, with ISO 27001 & ISO 20000 framework for failover and fall back to the appropriate DR site.

   DR drills needs to be performed by the MSP half yearly to check disaster preparedness. The Reverse replication from DR side to DC site also needs to be verified properly by the MSP.

   The testing should include the uninterrupted replication to DC servers & Data integrity test of DC servers. The MSP should address any lag in replication due to any unforeseen errors.

e. **Data Ownership**
   - DATA residing on the CSP/MSP datacenter will not be accessed, modified, deleted analyzed and Mined in any way or format by the CSP/MSP or by use of Artificial Intelligence without the explicit written consent of the department.

f. **Identity and Access Management for BCP**
   - Role based access to Department officials and Development team to carry out BCP.

5.3 Operational Acceptance tests

The MSP will have to facilitate the Operational Acceptance Tests. Operational acceptance tests will be performed by Department; however MSP will have to facilitate Operation Acceptance during commissioning of the system (or subsystem[s]), to ascertain whether the system (or major component or Subsystem[s]) conforms to the scope of work. The MSP will have to facilitate the testing of application from Department users during the Operational Acceptance. Necessary support shall be provided by the application vendor of Department.

5.4 Operations & Maintenance Services

The MSP shall be responsible for providing maintenance support from the date of issuance of operational acceptance by Department. The maintenance and support has been include following activities:

a. Resource Management
   i. Adequately size the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels
   ii. While the initial sizing & provisioning of the underlying infrastructure may be carried out based on the information provided by the Department, subsequently, it is expected that the MSP, based on the growth in the user load (peak and non-peak periods; year-on-year increase), has been scale up or scale down the compute, memory, and storage as per the performance requirements of the solution and meet the SLAs using the auto-scaling features.
   iii. In addition to auto-scaling, for any major expected increase in the workloads, carry out the capacity planning in advance to identify & provision, where necessary, the additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements of the solution
   iv. The scaling up / scaling down (beyond the auto-scaling limits or whenever the auto-scaling limits have to be changed) has to be carried out with prior approval by Department. The MSP should provide the necessary details including the sizing calculations, assumptions, current workloads & utilizations, expected growth / demand and any other details justifying the request to scale up or scale down. MSP is required to provision additional VM's when the utilization exceeds 80%.

b. Patch & Configuration Management

i. Manage the instances of storage, compute instances, and network environments. This includes Agency-owned & installed operating systems and other system software that are outside of the authorization boundary of the MSP. Service Provider is also responsible for managing specific controls relating to shared touch points within the security authorization boundary, such as establishing customized security control solutions. Examples include, but are not limited to, configuration and patch management, vulnerability scanning, disaster recovery, and protecting data in transit and at rest, host firewall management, managing credentials, identity and access management, and managing network configurations. Any required version/Software /Hardware upgrades, patch management etc. at the Cloud Site has been be supported by the solution provider for the entire contract period at no extra cost to DIT.

c. User Administration

i. Implement Identity and Access Management (IAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks.

ii. Administration of users, identities and authorizations, properly managing the root account, as well as any Identity and Access Management (IAM) users, groups and roles they associated with the user account

iii. Implement multi-factor authentication (MFA) for the root account, as well as any privileged Identity and Access Management accounts associated with it

d. Security Administration

i. Appropriately configure the security groups in accordance with Department's networking policies

ii. Regularly review the security group configuration and instance assignment in order to maintain a secure baseline.

iii. Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.

iv. Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity.

v. Properly implementing anti-malware and host-based intrusion detection systems on their instances, as well as any required network-based intrusion detection systems in accordance with the GoI/GoM's policies.

vi. Conducting regular vulnerability scanning and penetration testing of the systems, as mandated by GoI/GoM's policies.

vii. Review the audit logs to identify any unauthorized access to DIT's systems.

viii. The service provider shall conduct vulnerability and penetration test (from a third party testing agency which may be CERT-IN empanelled) on the proposed Cloud solution in every 6 months and reports should be shared.

ix. The MSP needs to update the system in response to any adverse findings in the report, without any additional cost to Department. Department may also depute auditors to conduct security check/ vulnerability test/penetration test.

e. Monitoring Performance and Service Levels

i. Provide and implement tools and processes for monitoring the availability of assigned applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues

ii. Reviewing the service level reports, monitoring the service levels and identifying any deviations from the agreed service levels

iii. Monitoring of service levels, including availability, uptime, performance, application specific parameters, e.g. for triggering elasticity, request rates, number of users connected to a service

iv. Detecting and reporting service level agreement infringements

v. Monitoring of performance, resource utilization and other events such as failure of service, degraded service, availability of the network, storage, database systems, operating Systems, applications, including API access

vi. Necessary tools to monitor the root cause for performance degradation of any applications. User Department should be able to easily justify whether issue is actually an Application issue or Hosting/hardware/Bandwidth issue.

f. Usage Reporting and Billing Management

i. Track system usage and usage reports

ii. Monitoring, managing and administering the monetary terms of SLAs and other billing related aspects

iii. Provide the relevant reports including real time as well as past data/information/reports for user Department and DIT to validate the billing and SLA related penalties

iv. The following is only an indicative list of MIS reports that may be submitted to DIT:

Daily reports

- Summary of resolved, unresolved and escalated issues / complaints
- Log of backup and restoration undertaken

Weekly reports

- Summary of systems rebooted.
- Summary of issues / complaints logged with the OEMs.
- Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.
- Hypervisor patch update status of all servers including the Virtual Machines running

- Monthly reports
    - Component wise server as well as Virtual machines availability and resource utilization
    - Consolidated SLA / Non- conformance report. Summary of component wise uptime.
    - Log of preventive / scheduled maintenance undertaken Log of break-fix maintenance undertaken
    - All relevant reports required for calculation of SLAs

- Quarterly reports
    - Consolidated component-wise availability and resource utilization
    - All relevant reports required for calculation of SLAs

The MIS reports shall be in-line with the SLAs and the same shall be scrutinized by the DIT

g. Backup and restore

    i. Configure, schedule, monitor and manage backups of all the data including but not limited to files, images and databases as per the policy finalized by DIT.
    ii. Restore from the backup on monthly basis and on request where required

h. Business Continuity Services

    i. Provide business continuity services in case the primary site becomes unavailable

i. Support for third party audits
    i. Enable the logs and monitoring as required to support for third party audits

j. Connectivity
Provide on demand minimum 10 GBPS MPLS connectivity between Department and other CSPs/MSPs/DR site for portability and interoperability of applications of Departments and for use during BCP.

5.5. Management / Transition-Out Services

a. Provide a comprehensive exit management plan, with focus on sustainability

b. Migration of the VMs, data, content and any other assets to the new environment or on alternate Managed Service Provider's offerings and ensuring successful deployment and running of user Department's solution on the new infrastructure by suitably retrieving all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to Agency supplied industry standard media

c. Ensure that all the documentation required for smooth transition including configuration documents are kept up to date
d. Once the exit process is completed, remove the data, content and other assets from the cloud environment and destroy the VM, Content and data of user Department.

SECTION 6
Mandatory compliance requirements
(As specified in MeitY RFP for empanelment of CSP)

The compliance must be maintained on an on-going basis in order to retain the empanelment status. The CSPs has been have to retain the empanelment status with DIT. The mandatory requirements for the respective services in this section also form the minimum scope of work of the empanelled cloud service providers when offering cloud services to the end user departments.

The empanelled cloud service providers has been have to comply with the guidelines & standards specified by DIT at the time of their empanelment with DIT. CSP is responsible for all costs associated with implementing, assessing, documenting and maintaining the empanelment.

The empanelled cloud service offerings must comply with the additional guidelines / standards as and when such guidelines / standards are published by DIT at no additional cost to retain the empanelment status. Cloud Service Providers has been be given sufficient time and notice period to comply with the additional guidelines / standards. Any downtime during such upgrades has been not be factored for SLA calculations.

6.1. General Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. Shall be in accordance with the requirements in this application document.
2. There should be sufficient headroom (at an overall level in the compute, network and storage capacity offered) available for near real time provisioning (as per the SLA requirement of the Government Department) during any unanticipated spikes in the user load. The provisioning / de-provisioning SLAs may differ for the different cloud deployment models.
3. Ability to integrate fully with the Government of India approved Certificate Authorities to enable the Government Departments use the Digital Certificates / Digital Signatures.
4. The respective Government Department shall retain ownership of any user created/loaded data and applications hosted on CSP's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time.
5. The respective Government Department retains ownership of all virtual machines, templates, clones, and scripts/applications created for the department's application. The respective Government Department retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time.
6. The respective Governmnt Department retains ownership of Department loaded software installed on virtual machines and any application or product that is deployed on the Cloud by the Government Department.

7. The respective Government Department shall be provided access rights (including the underlying secure connection) to the user administration / portal of cloud services to have visibility into the dashboard, SLAs, management reports, etc. provided by the Cloud Service provider.
8. CSP shall not provision any unmanaged VMs for the applications.
9. CSPs shall provide interoperability support with regards to available APIs, data portability etc., for the Government Department to utilize in case of Change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.
10. Should adhere to the ever evolving guidelines as specified by CERT-In (http://www.cert-in.org.in/)
11. Should adhere to the relevant standards published (or to be published) by DIT or any standards body setup / recognized by Government of India and notified to the CSP by DIT as a mandatory standard.
12. CSP shall also adhere to the relevant audit requirements as defined in the application document.
13. The empanelled cloud service offerings has been have to comply with the guidelines & standards as and when such guidelines / standards are published by DIT within the timeframe given by DIT. CSP is responsible for all costs associated with implementing, assessing, documenting and maintaining the empanelment.
14. The empanelled cloud service offerings must comply with any additional guidelines / standards (applicable for the Empanelled Cloud Service Offerings) as and when such guidelines / standards are published by DIT at no additional cost to retain the empanelment status. Cloud Service Providers has been be given sufficient time and notice period to comply to the additional guidelines / standards. Any downtime during such approved upgrades has been be considered as approved downtime for SLA calculations.
15. DIT has been have the option to extend the Empanelment duration on expiry, to avail the services of the CSP for continuation of the services without the need to go for a separate empanelment process. The duration of extension has been be decided by DIT and has been be up to a maximum of one year. The decision on the extension has been be taken exclusively by Government Department keeping in consideration a) satisfactory performance of the Agency b) time constraints or other serious impediments in initiation c) technological reasons d) Where circumstances inescapably require taking recourse to this option.

6.2. Service Management and Provisioning Requirements

The below mandatory requirements are applicable for all cloud deployment models.

Service Management and Provisioning requirements address the technical requirements for supporting the provisioning and service management of the Cloud Service Offerings proposed to be empanelled. Service provisioning focuses on capabilities required to assign services to users, allocate resources, and services and the monitoring and management of these resources.

6.2.1. Service Provisioning

a) Provide the ability to provision virtual machines, storage and bandwidth dynamically (or on-demand), on a self-service mode or as requested.

b) Enable Service Provisioning via online portal/interface (tools).

c) Enable Service Provisioning via Application Programming Interface (API).

a) Secure provisioning, de-provisioning and administering [such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or Secure Shell (SSH)]

b) Support the terms of service requirement of terminating the service at any time (on-demand).

c) Provide a webpage and associated Uniform Resource Locator (URL) that describes the following:

Service Level Agreements (SLAs)

Help Desk and Technical Support

Resources (Documentation, Articles/Tutorials, etc)

d) Make the Management Reports described in this application document accessible via online interface. These reports shall be available for one year after being created.

e) The CSP is expected to carry out the capacity planning in advance to identify & provision, where necessary, the additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements of the solution. There should not be any constraints on the services.

f) The CSP shall ensure that effective Remote Management features exist so that issues can be addressed by the Government Department in a timely and effective manner.

g) Service Provisioning shall be available with two factor authentication via the SSL through web browser.

6.2.2. Service Level Agreement Management

h) Provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime of 99.5%, SLA measured at the VM Level & SLA measured at the Storage Levels

i) Document and adhere to the SLAs to include:

Service Availability (Measured as Total Uptime Hours / Total Hours within the Month) displayed as a percentage of availability up to one-tenth of a percent (e.g. 99.5%)

Within a month of a major outage occurrence resulting in greater than 1-hour of unscheduled downtime. Describe the outage including description of root-cause and fix.

Service provisioning and de-provisioning times (scale up and down) in near real- time should be as per the SLA requirement of the Government Department. The provisioning / de-provisioning SLAs may differ for the different cloud deployment models.

j) Helpdesk and Technical support services to include system maintenance windows

1) CSP shall implement the monitoring System including any additional tools required for measuring and monitoring each of the Service Levels as per the SLA between the Government Department and the CSP.

6.2.3. Operational Management

1. Manage the network, storage, server and virtualization layers, to include performance of internal technology refresh cycles applicable to meet the SLAs
2. Provide a secure, dual factor method of remote access which allows the Government Department designated personnel (privileged users) the ability to perform duties on the hosted infrastructure
3. Upgrade and periodically replace hardware without financial impact to the Government Department. All the data within it shall be immediately deleted/destroyed and certify the VM and data destruction to the Government Department as per stipulations and shall ensure that the data cannot be forensically recovered.
4. Perform patch management appropriate to the scope of their control and/or Provide self-service tools to perform patch management
    a. Alerts well in advance on the upcoming patches via email and management portal.
    b. Patch VMs on the next available patch management change window and / or provide self-service tools to patch VMs.
    c. Application of automated OS security patches (where OS is the responsibility of the CSP) and / or provide self-service tools for application of OS security patches.
    d. Send regular reminders to the end user Department designated email address five (5) days prior to patch cut-off dates
5. OS level vulnerability management – all OS images created within the cloud platform are regularly patched with the latest security updates or the latest security updates are available to the Government Department along with the self-service tools to apply the patches as per the requirement of the Government Department.
6. Provide the artifacts, security policies and procedures demonstrating its compliance with the Security Assessment and Authorization requirements as described in Security Requirements in this application document.
7. Monitor availability of the servers, CSP -supplied operating system & system software, and CSP’s network
8. The CSP is fully responsible for tech refreshes, patch management and other operations of infrastructure that is in the scope of the CSP.
9. Investigate outages, perform appropriate corrective action to restore the hardware, operating system, and related tools

1) CSP should manage CSP provisioned infrastructure including VMs as per the ITIL standards.
2) Comply with technology refresh requirements as required so as to upgrade any technology prior to reaching end of life / end of support and as well as to ensure security requirements and service level agreements (SLA) are met.
3) Software (limited to OS, security solutions and other platform stack where offered by the CSP to the Government Department) has been never be more than two versions behind unless deferred or rejected by Government Department. This is not applicable to software such as cloud management stack (provisioning, orchestration and metering, etc.).

6.2.4. Data Management

a) Manage data isolation in a multi-tenant environment.
b) The CSP should provide tools and mechanism to the Government Department or its appointed agency for defining their backup requirements & policy.
c) The CSP should provide tools and mechanism to the Government Department or its appointed agency for configuring, scheduling, performing and managing back-ups and restore activities (when required) of all the data including but not limited to files, folders, images, system state, databases and enterprise applications in an encrypted manner as per the defined policy.
d) Transfer data back in-house either on demand or in case of contract or order termination for any reason
e) Manage data remanence throughout the data life cycle.
f) Provide and implement security mechanisms for handling data at rest and in transit.
g) CSP shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Government Department.
h) When the Government Department or CSP (with prior approval of the Government Department) scales down the infrastructure services, CSP is responsible for deleting or otherwise securing Government Department's Content/data prior to VM deletion and in case deleted, shall ensure that the data cannot be forensically recovered.

6.3. User/Admin Portal Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. Utilization Monitoring

Provide automatic monitoring of resource utilization and other events such as failure of service, degraded service, etc. via service dashboard or other electronic means.
Real time performance thresholds

Real time performance health checks

Real time performance monitoring & Alerts

Historical Performance Monitoring

Capacity Utilization statistics

Cloud Resource Usage including increase / decrease in resources used during auto-scale

2. Trouble Management -
   a. Provide Trouble Ticketing via online portal/interface (tools).
3. User Profile Management
   a. Support maintenance of user profiles and present the user with his/her profile at the time of login

6.4. Integration Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. Provide support to all Application Programming Interfaces (APIs) including REST API that CSP develops/provides.

6.5. LAN / WAN Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. Local Area Network (LAN) shall not impede data transmission..
2. Provide a redundant local area network (LAN) infrastructure and static IP addresses from customer IP pool or "private" non-internet routable addresses from CSP pool.
3. Ability to deploy VMs in multiple security zones, as required for the project, defined by network isolation layers in the Customer's local network topology
4. Provide access to Wide Area Network (WAN)
5. Provide private connectivity between a Government Department's network and Data Center Facilities
6. IP Addressing:
   a. Provide IP address assignment, including Dynamic Host Configuration Protocol (DHCP).
   b. Provide IP address and IP port assignment on external network interfaces.
   c. Provide dedicated virtual private network (VPN) connectivity.
   d. Allow mapping IP addresses to domains owned by the Government Department, allowing websites or other applications operating in the cloud to be viewed externally as Government URLs and services.
7. Provide infrastructure that is IPv6 compliant.

8. CSP shall support for providing the secure connection to the Data Center and Disaster Recovery Center (where applicable) from the Government Department Offices.
9. The data center and disaster recovery centre facilities (where applicable) should support connection to the wide area network through high bandwidth links of appropriate capacity to take care of the needs of various types of user entities. Provision has to be made for segregation of access path among various user categories.
10. Support dedicated link to the offices of the Government Department to access the data center and a separate internet link for the other external stakeholders to get access to Government Department services.
11. CSP shall have the capability to provide adequate bandwidth between Primary Data Center and Disaster Recovery Center for data replication purpose.
12. Support network level redundancy through MPLS lines from two different service providers, alternate routing paths facilitated at ISP backbone (MPLS), redundant network devices etc. These two network service providers should not share same back end infrastructure. Redundancy in security and load balancers, in high availability mode, has been be provided to facilitate alternate paths in the network

6.6. Data Center Facilities Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. The data center facilities shall cater for the space, power, physical infrastructure (hardware).
2. The data center facilities and the physical and virtual hardware should be located within India
3. The space allocated for hosting the infrastructure in the Data Center should be secure.
4. The Data Center should be certified for the latest version of ISO 27001 (year 2013) and provide service assurance and effectiveness of Management compliant with SSAE 16 / ISAE 3402 standards
5. The NOC and SOC facility must be within India for the Cloud Environments and the managed services quality should be certified for ISO 20000:1.
6. CSP should comply to Cloud Security ISO Standard ISO 27017:2015, Privacy Standard ISO 27018:2015
7. The Data Center should conform to at least Tier III standard (preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party) and implement tool-based processes based on ITIL standards
8. All the physical, environmental and security features, compliances and controls of the Data Center facilities (as required under this application document) shall be enabled for the environment used for offering cloud services.

9. Provide staff, technical and supervisory, in sufficient numbers to operate and manage the functioning of the DC & DRC with desired service levels
10. The data center should comply with the Physical Security Standards as per the latest version of ISO 27001 (year 2013) standards.

6.7. Cloud Storage Service Requirements

The below mandatory requirements are applicable for all cloud deployment models.

The service shall be available online, on-demand, and dynamically scalable up or down per request for service from the end users (Government Department or Government Department's nominated agencies) with two factor authentication via the SSL through a web browser.

1. Service shall provide scalable, redundant, dynamic storage
2. Service shall provide users with the ability to procure storage with two factor authentication via the SSL through a web browser and manage storage capabilities remotely via the SSL VPN clients as against the public internet.
3. Service shall provide storage capabilities on-demand, dynamically scalable per request and management of the storage via the SSL VPN clients as against the public internet
4. Storage Space: Online, on-demand virtual storage supporting a single storage sizes in multiples of 1 GB
5. Data Transfer Bandwidth: Bandwidth utilized to transfer files/objects in/out of the providers infrastructure supporting a minimum of 100GB of data transferred (in and out) within 1 hour via the network
6. There shall not be any additional costs associated with data transfer over and above the ordinary bandwidth charges, or for bulk transfer for Government Department.

6.8. Virtual Machine Requirements

The below mandatory requirements are applicable for all cloud deployment models.

The service shall be available online, on-demand and dynamically scalable up or down per request for service from the end users (Government Department or Government Department's nominated agencies) with two factor authentication via the SSL through a web browser.

1. Service shall provide auto-scalable, redundant, dynamic computing capabilities or virtual machines.
2. Service shall allow Government Department authorized users to procure and provision computing services or virtual machine instances online with two factor authentication via the SSL through a web browser.

3. Service shall allow users to securely and remotely load applications and data onto the computing or virtual machine instance from the SSL VPN clients only as against the public internet.
4. Perform an Image backup of Customer VM Image information or support the ability to take an existing running instance or a copy of an instance and export the instance into a Government Department's approved image format.
5. Configuration and Management of the Virtual Machine shall be enabled via a Web browser over the SSL VPN clients only as against the public internet
6. In case of suspension of a running VM, the VM shall still be available for reactivation for a reasonable time without having to reinstall or reconfigure the VM for the Government Department solution. In case of suspension beyond a reasonable time, all the data within it shall be immediately deleted / destroyed and certify the VM and data destruction to the Government Department as per stipulations and shall ensure that the data cannot be forensically recovered.
7. CSP shall ensure that VMs receive OS patching, health checking, Systematic Attack Detection and backup functions.
8. Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network
9. CPU (Central Processing Unit) - CPU options shall be provided as follows:
   A minimum equivalent CPU processor speed of 2.4GHz shall be provided.
   The CPU shall support 64-bit operations
10. Provide hardware or software based virtual load balancer Services (VLBS) through a secure, hardened, redundant CSP Managed Virtual Load Balancer platform
11. Provide hardware or software based virtual load balancing as a service to provide stateful failover and enable Customers to distribute traffic load across multiple servers.
12. Support Clustering
13. Operating System (OS)
    a. Service shall support one or more of the major OS such as Windows, LINUX.
    b. Management of the OS processes and log files including security logs retained in guest VMs;
    c. Provide anti-virus protection;
    d. Provide OS level security as per CSP standard operational procedures as defined in the Information Security Controls for Cloud Managed Services and supporting documentation;
14. Persistence
    a. Persistent Bundled Storage is retained when the virtual machine instance is stopped or

b. Non-Persistence – Non-Persistence Bundled Storage is released when the virtual instance is stopped. If quoting Non-Persistence VM, the CSP shall provide VM Block storage

15. RAM (Random Access Memory): Physical memory (RAM) reserved for virtual machine instance or Computing supporting a minimum of 1GB of RAM. Memory (RAM) requirement should be different for different type of servers such as web servers and database servers.
16. Disk Space options allocated for all virtual machines and file data supporting a minimum of 40GB bundled storage.
17. Virtual Machine Block Storage Service Requirements
    a. Service shall provide scalable, redundant, dynamic Web-based storage
    b. Service shall provide users with the ability to procure and provision block storage capabilities for cloud virtual machines remotely with two factor authentication via the SSL through a web browser.
    c. Service shall provide block storage capabilities on-demand, dynamically scalable per request for virtual machine instances.
    d. Block Storage – Once mounted, the block storage should appear to the virtual machine like any other disk
    e. Storage Space: Online, on-demand storage volumes of arbitrary size ranging from 1 GB to at least 1 TB
    f. Input/output (I/O) Requests: Input/output requests on block storage
18. Government Department retains ownership of all virtual machines, templates, clones, and scripts/applications created for the Department's application
19. Government Department retains the right to request full copies of these virtual machines at any time.
20. Government Department retains ownership of Department loaded software installed on virtual machines and any application or product that is deployed on the Cloud by the Government Department.
21. Support a secure administration interface - such as SSL/TLS or SSH - for the Government Department designated personnel to remotely administer their virtual instance
22. Provide the capability to dynamically allocate virtual machines based on load, with no service interruption
23. Provide the capability to copy or clone virtual machines for archiving, troubleshooting, and testing
24. Cloud provider should offer fine-grained access controls including role based access control, use of SSL certificates, or authentication with a multi-factor authentication.

25. Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.
26. Government Department should be permitted to bring and upload additional properly licensed non-operating system software for operation in cloud as required for the Government Department solution for use within the Services by installing it directly on a VM.
27. RAM or CPU of virtual machine should scale automatically whenever there is spike in load to deliver application availability even during spike in load.
28. Provide facility to configure virtual machine of required vCPU, RAM and Disk.
29. Provide facility to use different types of disk like SAS, SSD based on type of application.

6.9. Disaster Recovery & Business Continuity Requirements

CSP is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data center of the Government Department and meet the RPO and RTO requirements. RPO should be less than or equal to 2 hours and RTO shall be less than or equal to 4 hours. The key transaction data shall have RPO of 15 minutes. However, during the change from Primary DC to DRC or vice-versa (regular planned changes), there should not be any data loss. There shall be asynchronous replication of data between Primary DC and DRDC and the CSP has been be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements.

1. The Primary DC (of the Government Department) and the DRC should be in different seismic zones

2. During normal operations, the Primary Data Center (of the Government Department) has been serve the requests. The Disaster Recovery Site has been not be performing any work but has been remain on standby. During this period, the compute environment for the application in DR shall be available but with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Center site.

3. In the event of a site failover or switchover, DR site has been take over the active role, and all requests has been be routed through that site. Application data and application states has been be replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO. This is the period during which the Compute environment for the application shall be equivalent to DC. The installed application instance and the database shall be usable and the same SLAs as DC shall be provided. The use of this Full Compute DR environment can be for specific periods during a year for the purposes of DC failure or DR Drills or DC maintenance. The Database and storage shall be of full capacity and the licenses and security shall be for full infrastructure. The bandwidth at the DR shall be scaled to the level of Data center. Users of application should be routed seamlessly from DC site to DR site. The CSP shall conduct DR drill for two days at the interval of every six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site. However, during the change from DC to DRC or vice-versa (regular planned changes), there should not be any data loss.

4. The CSP shall clearly define the procedure for announcing DR based on the proposed DR solution. The CSP shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The CSP shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Department at least two weeks before such drill.
5. The CSP should offer dashboard to monitor RPO and RTO of each application and database.

6. The CSP should offer switchover and switchback of individual applications instead of entire system.

7. Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to respective authorities.

6.10. Security Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. CSP is responsible for provisioning, securing, monitoring, and maintaining the hardware, network(s), and software that support the infrastructure and present Virtual Machines (VMs) and IT resources to the Government Department. On its part, the Government Department is responsible for the security of the "guest" Operating System (OS) and any additional software, up to and including the applications running on the guest OS.

2. In case, the CSP provides some of the System Software as a Service for the project, CSP is responsible for securing, monitoring, and maintaining the System and any supporting software. Government Department is responsible for securing and maintaining the Government Department application.
3. The Data Center Facility shall at a minimum implement the security toolset: Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Multi Factor Authentication, VPN, IPS, Log Analyzer / Syslog, SSL, DDOS Protection, HIDS / NIDS, Rights Management, SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting)
4. Meet the ever evolving security requirements as specified by CERT-In (http://www.cert-in.org.in/)
5. Compliance to Cloud Security ISO Standard ISO 27017:2015, Privacy Standard ISO 27018:2015 and ISO 20000:9
6. Meet any security requirements published (or to be published) by DIT or any standards body setup / recognized by Government of India from time to time and notified to the CSP by DIT as a mandatory standard
7. DIT and Government Department reserves the right to verify the security test results.
    a. In case of the Government Community Cloud, DIT and Government Department reserves the right to verify the infrastructure.
8. Implement industry standard storage strategies and controls for securing data in the Storage Area Network so that clients are restricted to their allocated storage.
9. Deploy public facing services in a zone (DMZ) different from the application services. The Database nodes (RDBMS) should be in a separate zone with higher security layer.
10. Ability to create non-production environments and segregate (in a different VLAN) non-production environments from the production environment such that the users of the environments are in separate networks.
11. Cloud offering should have built-in user-level controls and administrator logs for transparency and audit control
12. Cloud Platform should be protected by fully-managed Intrusion detection system using signature, protocol, and anomaly based inspection thus providing network intrusion detection monitoring.
13. Cloud platform should provide Edge-to-Edge security, visibility and carrier-class threat management and remediation against security hazards like Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, botnets, etc. Also, shall provide protection against network issues such as traffic and routing instability.

14. Cloud platform should provide Web Application Filter for OWASP Top 10 protection as a service that can be enabled for Government Departments that require such a service.
15. Access to Government Department provisioned servers on the cloud should be through SSL VPN clients only as against the public internet.
16. Provision of private network ports to be connected to Government Department network for additional secure connectivity between Government Department network and the cloud through support for MPLS, Fiber, P2P links.

17. Virtual Machines should not have console access.
18. Cloud Service provider shall allow audits of all administrator activities performed by Government Department and allow Government Department to download copies of these logs in CSV format.
19. Maintain the security features described below, investigate incidents detected, undertake corrective action, and report to Government Department, as appropriate
20. Deploy and update commercial anti-malware tools (for systems using Microsoft operating systems), investigate incidents, and undertake remedial action necessary to restore servers and operating systems to operation.

21. Shall provide consolidated view of the availability, integrity and consistency of the Web/App/DB tiers
22. CSP should enforce password policies (complex password, change password in some days etc)
23. Shall be contractually subject to all GoI IT Security standards, policies, and reporting requirements. The CSP shall meet and comply with all GoI IT Security Policies and all applicable GoI standards and guidelines, other Government-wide laws and regulations for protection and security of Information Technology.

24. Shall generally and substantially and in good faith follow GoI guidelines and CERT-In and DIT Security guidance. Where there are no procedural guides, use generally accepted industry best practices for IT security.
25. Information systems must be assessed whenever there is a significant change to the system’s security posture
26. Conduct regular independent third party assessments of the CSP’s security controls to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements and submit the results to DIT and Government Department

27. In case CSP has industry standard certifications (assessed by a third party auditor) that verify compliance against the security requirements of the application document, SLA & MSA, the results, relevant reports, certifications may be provided with evidence along with the mapping of the industry standard certification controls against the application document requirements. However, if there are any requirements that do not fall under the industry standard certifications, the CSP shall get the Third Party Auditor to assess the the conformance to the requirements.
28. Provide an independent Security Assessment/Risk Assessment
29. DIT reserves the right to perform Penetration Test. If the DIT exercises this right, the CSP shall allow DIT's designated third party auditors to conduct activities to include control reviews that include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of Department's information. This includes the general support system infrastructure.
30. Identified gaps shall be tracked for mitigation in a Plan of Action document.
31. CSP is responsible for mitigating all security risks found and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government has been determine the risk rating of vulnerabilities.
32. Shall provide access to the DIT or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. DIT reserves the right to conduct on-site inspections. CSP shall make appropriate personnel available for interviews and documentation during this review. If documentation is considered proprietary or sensitive, these documents may be reviewed on-site under the CSP's supervision.
33. Shall provide vulnerability scan reports from Web Application, Database, and Operating System Scans or the services for the Government Department to run the vulnerability scan. Scan results (that fall under the scope of the CSP) shall be managed and mitigated in Plans of Action.
34. All documents exclusively produced for the project are the property of the Government Department and cannot be reproduced, or retained by the CSP. All appropriate project documentation has been be given to Government Department during and at the end of this contract or at the time of termination of the contract. The CSP shall not release any project information without the written consent of the Government Department. Any request for information relating to the Project presented to the CSP must be submitted to the Government Department for approval.

35. CSP shall protect all Government Department data, equipment, etc., by treating the information as sensitive. Sensitive but unclassified information, data, and/or equipment has been only be disclosed to authorized-personnel. The CSP shall keep the information confidential, use appropriate safeguards to maintain its security in accordance with minimum standards. When no longer required, this information, data, and/or equipment shall be returned to Government Department control, destroyed, or held until otherwise directed by the Government Department. The CSP shall destroy unneeded items by burning, shredding, or any other method that precludes the reconstruction of the material.
36. DIT has the right to perform manual or automated audits, scans, reviews, or other inspections of the CSP's IT environment being used to provide or facilitate services for the Government Department through a DIT's designated third party auditor. CSP shall be responsible for the following privacy and security safeguards:
    a. CSP shall not publish or disclose in any manner, without the DIT's written consent, the details of any safeguards either designed or developed by the CSP under the Agreement or otherwise provided by the GoI & Government Department.
    b. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the CSP, the CSP shall afford the DIT logical and physical access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods:
        i. Authenticated and unauthenticated operating system/network vulnerability scans
        ii. Authenticated and unauthenticated web application vulnerability scans
        iii. Authenticated and unauthenticated database application vulnerability scans
37. Automated scans can be performed by DIT's designated third party auditors, using DIT specified tools. If the CSP chooses to run its own automated scans or audits, results from these scans may, at the DIT's discretion, be accepted in lieu of DIT performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the DIT. In addition, the results of CSP-conducted scans shall be provided, in full, to the DIT.
38. Submission to regular audits: CSP has been submit to regular audits commissioned by DIT. The purpose of these audits has been not only be to ensure conformance with the requirements stated in this application document, but also to ensure that the implementation is executed in the best of ways to meet the requirements of DIT. These audits may be conducted by DIT or DIT's designated third party auditors. CSP has been cooperate fully with the auditor. DIT has been inform the CSP of the short-comings if any after the audit is completed; and the CSP has been respond appropriately and address the identified gaps.

6.11. Legal Compliance Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. IT Act 2000 (including 43A) and amendments thereof
2. Meet the ever evolving security requirements as specified by CERT-In (http://www.cert-in.org.in/)
3. Meet any security requirements published (or to be published) by DIT or any standards body setup / recognized by Government of India from time to time and notified to the CSP by DIT as a mandatory standard
4. All services acquired under this application document including data has been be guaranteed to reside in India only.
5. There shall not be any legal frameworks outside Indian Law applicable to the operation of the service (and therefore the information contained within it).
6. A copy of the contract / MOU (excluding the commercials) between CSP & Government Department for the purpose of the project, aligned to the terms & conditions of the application document, should be provided to DIT, as and when requested by DIT.
7. DIT has initiated the process of identification of the Standards, develop the necessary specifications, frameworks and guidelines including the guidelines for empanelment of cloud service offerings with the help of a Cloud Management Office (CMO). The guidelines may also include continuous monitoring of the shared systems that can be leveraged by Government to both reduce their security compliance burden and provide them highly effective security services.
    a. The empaneled cloud service offerings has been have to comply with the guidelines & standards as and when such guidelines / standards are published by DIT within the timeframe given by DIT.
    b. CSPs should be prepared to submit the necessary artifacts and the independent verification within the timeframe determined by DIT once the guidelines & standards are published by DIT.
    c. CSP is responsible for all costs associated with implementing, meeting, assessing, documenting and maintaining the empanelment.
    d. The cost of meeting all requirements, getting empaneled and maintaining empanelment is the responsibility of CSP.
    e. If the CSP fails to meet the guidelines & standards as set by GoI within the timeframe set by DIT, the Government Department reserves the right to terminate the contract and request to move to a different CSP that meets the mandatory guidelines & standards at no additional cost to Government Department. The Exit Management provisions shall come into effect in such a scenario.

8. CSP shall be responsible for the following privacy and security safeguards:
    a. CSP shall not publish or disclose in any manner, without the Government Department's written consent, the details of any safeguards either designed or developed by the CSP under the agreement or otherwise provided by the Government Department or Government of India.
    b. CSP shall adhere to the privacy safeguards as laid down by the DIT and Government Department.
    c. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the CSP, the CSP shall afford the DIT or its nominated agency access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases.
    d. If new or unanticipated threats or hazards are discovered by either the DIT or Government Department, Government or the CSP, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of CERT-In and the other party.

6.12.a Management Reporting Requirements

The below mandatory requirements are applicable for all cloud deployment models.

Deliverables listed below should be accessible via online interface not later than 10 days after the end of the calendar month and available for up to one year after creation. The information shall be available in format approved by DIT. The CSP shall monitor and maintain the stated service levels as agreed in the Service Level Agreement between the Government Department and the CSP.

1. Service Level Management
    a. Service Level Management Reports (as per the service levels agreed in the Service Level Agreement between the Government Department and the CSP)
    b. Service Availability at the VM & Service Availability at the Storage Level (Measured as Total Uptime Hours / Total Hours within the Month) displayed as a percentage of availability up to one-tenth of a percent (e.g. 99.5%)
    c. Text description of major outages (including description of root-cause and fix) resulting in greater than 1-hour of unscheduled downtime within a month
2. Network and Security Administration (including security breaches with classification, action taken by the CSP and current status) related reports

3. Help Desk / Trouble Tickets raised by the DIT and / or Government Department
    a. Number of Help Desk/customer service requests received.
    b. Number of Trouble Tickets Opened
    c. Number of trouble tickets closed
    d. Average mean time to respond to Trouble Tickets (time between trouble ticket opened and the first contact with customer)
    e. Average mean time to resolve trouble ticket
4. Monthly utilization (including peak and non-peak volumetric details) of the Service Offerings for the respective Government Department
5. Centralized Monitoring & Management and Reporting with:
    a. Alerts on event threshold and policy based actions upon deviations.
    b. Internet & Intranet Data Transfer
    c. Virtual Instances (vCPU, vMemory, Storage and Network Port) configuration and utilization
    d. Storage Volume (Read/Write and IOPS)
    e. Load balancer
    f. Application Services
    g. Database Monitoring
    h. Reports on non-conformance and escalation for privileged access by unauthorized roles/ identities
6. Government Department has been have ten (10) business days, to review, accept or reject all deliverables. Any comments made by the Government Department shall be addressed and a revised deliverable submitted within five (5) business days after the receipt of the comments/rejection, unless a further time extension for incorporating the comments is approved by Government Department.
7. Third Party Audit Certification (at the cost of CSP) every six months indicating the conformance to the requirements detailed in this application document of the empaneled cloud service offerings which are being used by the Government Department. In case the empaneled cloud service offerings are not deployed for any Government Department, a self-certification every six months indicating the conformance to the requirements detailed in this application document, SLA & MSA of the environments & cloud service offerings empaneled should be provided to DIT
8. Any other reports as deemed required by DIT from time-to-time.

6.12.b Exit Management and Transition Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. Continuity and performance of the Services at all times including the duration of the Agreement and post expiry of the Agreement is a critical requirement of the Government Department. It is the prime responsibility of CSP to ensure continuity of service at all times of the Agreement including exit management period and in no way any facility/service shall be affected/degraded .Further, CSP is also responsible for all activities required to train and transfer the knowledge to the Replacement Agency (or Government Department) to ensure similar continuity and performance of the Services post expiry of the Agreement.
2. At the end of the contract period or upon termination of contract, CSP is required to provide necessary handholding and transition support to ensure the continuity and performance of the Services to the complete satisfaction of Government Department.
3. CSP shall support the Government Department in migration of the VMs, data, content and any other assets to the new environment created by the Government Department or any Agency (on behalf of the Government) on alternate cloud service provider's offerings to enable successful deployment and running of the Government Department's solution on the new infrastructure. CSP shall certify the VM, Content and data destruction to the Government Department as per stipulations and shall ensure that the data cannot be forensically recovered. CSP shall have the responsibility to support and assist the Government Department till the Department is able to successfully deploy and access the services from the new environment.
4. CSP shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Government Department.
5. During the exit/transition management process, it is the responsibility of the CSP to address and rectify the problems with respect to migration of the Department application and related IT infrastructure including installation/reinstallation of the system software etc.
6. The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with Government Department.
7. During the contract period, the CSP shall ensure that all the documentation required by the Government Department for smooth transition including configuration documents are kept up to date and all such documentation is handed over to the department during the exit management process.

6.13. Managed Services Requirements

Applicable only when one or a combination of IaaS, PaaS,DRaaS, DevOps and VDaaS cloud service offerings of the Cloud Service Provider (CSP) are proposed to be empaneled.

6.13.1. Backup Services

g. The CSP should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications as per the policy defined by DIT or the Government Department.

h. The CSP shall be responsible for file system and database backup and restore services. As part of the responsibilities the CSP should:

i. Perform and store data and file backups (process of duplicating the customers "to-be-backed-up" "Target Data") consisting of an initial full back up with daily incremental backups for files;

ii. For the files, perform weekly backups;

iii. For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files;

iv. Cloud platform should provide Encryption of all backup files and data and management of encryption keys as a service that can be enabled for Government Departments that require such a service.

v. Monitor and manage backup activity;

b. Restore the requested data with the objective to initiate a minimum of 95 percent of the total number of restore requests per calendar month within a two hour timeframe for data that can be restored from a local copy;

c. Retain inactive versions of backed up flat files for 30 days and the last version of a deleted file for 60 days;

d. Retain database backups for thirty (30) days;

e. Perform administration, tuning, optimization, planning, maintenance, and operations management for backup and restore;

f. Provide and install additional infrastructure capacity for backup and restore, as required; and,

g. Perform backup on the next scheduled backup window in case of any scheduling conflicts between backup and patch management.

6.13.2. Disaster Recovery & Business Continuity Services

1. In addition to the Primary DC, the CSP is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data center and meet the RPO and RTO requirements. RPO should be less than or equal to 2 hours and RTO shall be less than or equal to 4 hours. The key transaction data shall have RPO of 15 minutes. However, during the change from DC to DRC or vice-versa (regular planned changes), there should not be any data loss. There shall be asynchronous replication of data

between Primary DC and DRDC and the CSP has been be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements.

2. The Primary DC and the DRC should be in different seismic zones
3. The DRC can be offered from a traditional Data Center Facility and all the relevant mandatory requirements defined for the Primary Data Center as indicated below apply for the Disaster Recovery Center
   a. Deployment Model Specific Requirements as defined under Section 5.1
   b. General Requirements as defined under Section 5.2
   c. Service Level Agreement Management as defined under Section 5.3.2
   d. Operational Management as defined under Section 5.3.3
   e. Data Management as defined under Section 5.3.4
   f. User/Admin Portal Requirements under Section 5.4
   g. Integration Requirements under Section 5.5
   h. LAN / WAN Requirements under Section 5.6
   i. Data Center Facilities Requirements under Section 5.7
   j. Security Requirements under Section 5.11
   k. Legal Compliance Requirements under Section 5.12
   l. Management Reporting Requirements under Section 5.13
   m. Exit Management and Transition Requirements under Section 5.14
4. In case of any disaster, the security posture of the DR site shall be identical to the posture provided in the DC.
5. The disaster recovery site shall have the similar environment (physical & IT), processes, and controls (security, etc.) as that of the primary DC. During normal operations, the Primary Data Center has been serve the requests. The Disaster Recovery Site has been not be performing any work but has been remain on standby. During this period, the compute environment for the application in DR shall be available but with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Center site.
6. In the event of a site failover or switchover, DR site has been take over the active role, and all requests has been be routed through that site. Application data and application states has been be replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO. This is the period during which the Compute environment for the application shall be equivalent to DC. The installed application instance and the database shall be usable and the same SLAs as DC shall be provided. The use

of this Full Compute DR environment can be for specific periods during

i. year for the purposes of DC failure or DR Drills or DC maintenance. The Database and storage shall be of full capacity and the licenses and security shall be for full infrastructure. The bandwidth at the DR shall be scaled to the level of Data center. Users of application should be routed seamlessly from DC site to DR site. The CSP shall conduct DR drill for two days at the interval of every six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site. However, during the change from DC to DRC or vice-versa (regular planned changes), there should not be any data loss.

7. The CSP shall clearly define the procedure for announcing DR based on the proposed DR solution. The CSP shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The CSP shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Department at least two weeks before such drill.
8. The CSP should offer dashboard to monitor RPO and RTO of each application and database.
9. The CSP should offer switchover and switchback of individual applications instead of entire system.

Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to respective authorities.

****